Türkiye Ortadoğu Çalışmaları Dergisi
Turkish Journal of Middle Eastern Studies

ISSN: 2147-7523 E-ISSN: 2630-5631 Vol. 12, No. 2, 00-00, 2025
Publisher: Sakarya University DOI: https://doi.org/ 10.26513/tocd.1785938

Research Article

State Utilization of New Surveillance Technologies and Justification Strategies for the Public: A Case Study of Israel

Burak Şakir Şeker

Ankara Hacı Bayram Veli Üniversitesi, Ankara, Türkiye,
seker.burak@hbv.edu.tr
buraksakirseker@gmail.com

Abstract: This article examines the intricate relationship between state power, technological innovation, and social control, analyzing how states utilize emerging technologies, especially in surveillance and military capacities, and the legitimization strategies employed to justify these practices to both domestic and global audiences. A key observation is the dualism of state technology use, projecting beyond domestic control to external strategic and economic interests, demonstrating technology as both a commodity and diplomatic tool. Taking Israel as a conspicuous case study due to its peculiar geopolitical situation that has rendered the Palestinian territories a laboratory for innovative military and security technologies, this paper examines how combat-proven systems are created, internationally traded, making Israel's defense industry a leading sector. To understand these dynamics, the research integrates various theoretical frameworks including panopticism, dual-use technologies, securitization theory, constructivism, techno-authoritarianism, as well as theories pertaining to public opinion and state legitimation. The study starts by explaining the theoretical basis, its presence in Israel, and its global consequences. The study also considers the state's rationales founded upon security as well as humanitarian reasons, and includes a focus on international collusion as well as censorship in informing public opinion.

Keywords: State, Public Sphere, Surveillance, Israel, Digital Apartheid

Received: 17.09.2025
Accepted: 04.11.2025
Available Online: 24.11.2025

Introduction

The 21st century can be defined as a singular combination of fast-moving technology and heavy-handed government regulation, transforming politics, security and diplomacy. Governments are increasingly employing contemporary technologies in sensitive spots such as surveillance and warfare, and compelling legitimate questions concerning control, civilian rights, and institutional accountability are promptly generated. This convergence of technology and governance requires greater recognition of both the technical implementation and the multifaceted rationalizations furnished by national and supranational authorities for employing them.

Cite as (APA 7): Şeker B. Ş. (2025). State Utilization of New Surveillance Technologies and Justification Strategies for the Public: A Case Study of Israel. *Türkiye Ortadoğu Çalışmaları Dergisi*, 12(2), 00-00. https://doi.org/ 10.26513/tocd.1785938

The research examines a state's means of leveraging technology, in particular, global surveillance and global security initiatives. The study is equally concerned with legitimizing such initiatives at home and internationally. It broadens a classical conception of domestic security, highlighting technology as a point of emphasis in global politics as well as a predictor in terms of economic progress.

In a detailed analysis of the complex and multi-dimensions involved in the innovation and application of such technologies, this study tries filling a very significant gap—often referred by scholars as a lacuna (Sivakumar & Lukose, 2017)—in the literature. Furthermore, the study delves into the dynamic and vibrant interaction existing across domestic control measures and the implications for global relations and the pursuits for economic profit. In a break away from a very simplistic dichotomy, in which technology is simply and solely reduced to a facilitator for control, the approach here lies the focus on the significant role technologies play as commodities and assets in the global arena. Therefore, the work provides a novel examination of the subject matter at hand.

Israel's special geopolitical context bears special importance. For decades, this setting has converted the Gaza Strip and West Bank into a research ground for new warfare and security equipment. Employed equipment achieves a global status as tested in battle or combat-proven, which makes Israel's defense sector a trendsetter. The financial advantages point out that these ‘lab experiments’ are a calculated, lucrative venture, not a by-product of war.

This research adopts a qualitative and interpretive method using a single-case study of Israel to explore state use and legitimization of surveillance technologies. The analysis relies on secondary sources such as government statements, international reports, and scholarly literature. The study employs document analysis and critical discourse analysis to interpret how these texts construct narratives of security, legitimacy, and technological innovation. Through qualitative content analysis, recurring justifications, metaphors, and legitimizing frames are identified and connected to theoretical frameworks including panopticism, securitization theory, and constructivism. This approach allows for a holistic understanding of how technological governance is rationalized in political and moral terms, both domestically and internationally.

This study first develops a theoretical framework covering the concepts of panopticism, securitization theory, constructivism, techno-authoritarianism, dual-use technologies and concepts related to public opinion and state legitimacy. The paper then proceeds to examine the application of such theories in the Israeli context, and subsequently a detailed exploration of the phenomenon of the

'Palestinian laboratory,' the interface of state intelligence communities and private sectors, and the distinct control technologies by which digital apartheid[1] is articulated. Furthermore, it also addresses the modalities of employed legitimization strategies, the impact of global complicity and the control of narrative mechanisms. Thereafter, an exploration of the global international context is presented including the implications on universal norms and human rights.

Selected theories and concepts of state power and technology utilization

To properly understand how states handle emerging technologies and then report their actions to citizens, a number of competing frameworks for analysis deserve consideration. These conceptual frameworks will help shed light on the relations of power, control techniques, and how governments attain the acceptance, or at least the acquiescence, of citizens regarding what they undertake. When states adopt high technologies, particularly regarding monitoring and social control, it is possible to subject these practices to a set of theoretical terms.

Panopticism and the surveillance state

Michel Foucault's idea of "panopticism" (2008) offers a powerful way to think about modern surveillance. It started as Jeremy Bentham's (1843) design for a prison, where a central tower could observe all inmates without them knowing if they were being watched at any given moment. This setup creates a feeling of constant surveillance for prisoners. Because they know they might be observed, they start to watch themselves, essentially becoming their own guards. This architectural design becomes a machine for creating and sustaining a power relation independent of the person exercising it. In such a system, power does not rely on obvious force; instead it hinged on the subtle, widespread influence of being watched, which often leads people to censor themselves and conform.

The surveillance state (Foreign Policy, 2013) takes this idea and applies it to an entire society. It describes a society, where governments and other organizations use various technologies to watch and manage citizens' behavior. This shift from physical surveillance to digital tools is driven by new technologies, changing public attitudes about crime and safety, and the state's need to maintain control. Governments, law enforcement, private companies that develop and sell surveillance technologies, and the people under surveillance are all key players. The widespread nature of surveillance (Gouck, 2018) suggests that power can be effective even if surveillance is not continuous, as long as people feel they may be

observed at any time. This creates a system in which individuals are caught in a power dynamic that they themselves help sustain, showing a deep change in how control works.

Securitization theory and constructivism in international relations

Securitization theory, developed by the Copenhagen School, offers a way to understand how certain issues become matters of security (Wæver, 2011). It suggests that security is not something that just exists. Instead, it is created when a powerful figure or institution successfully frames an issue as an existential threat to something important, like the state or its people. This process then moves the issue beyond politics, making it acceptable to use extraordinary means that would otherwise be seen as out of line (Buzan & Wæver, 2009)

A crucial point of securitization is that its success does not necessarily depend on a real threat but on the ability to effectively imbue a development with a specific character through words and actions (Buzan et al., 1998). When an issue is successfully securitized, it attracts a disproportionate amount of attention and resources compared to other problems that might actually present a greater harm potential. This can lead to extraordinary measures such as declaring emergencies, mobilizing the military, or even international conflict. Securitization can further impede public debate in political or academic settings as the securitized subject narrows the limits of discourse. The theory often suggests that securitization can be a negative process, potentially undermining democratic practices and reducing scrutiny of those in power (Gad & Petersen, 2011).

Constructivism, as a way of thinking in international relations, highlights that the fundamental aspects of how countries interact are shaped by shared ideas and beliefs, rather than just by physical power or resources (Hopf, 1998). Unlike theories that see the international system as inherently chaotic, constructivists like Alexander Wendt (1992) argue that the rules and structures governing international relations are social creations. This means they are formed by ongoing social practices and interactions.

A core idea of constructivism is that shared ideas, beliefs, and identities are the main drivers of how people and groups associate with each other, and that the identities and interests of countries are shaped by these shared ideas. Reality itself is seen as something we build together through common meanings and understandings (Baldwin, 2016). Constructivist research looks at how the beliefs and actions of different players create the social world. It examines how norms and

identities influence what states care about and how they behave, and how these things can change through social interaction and learning (Shadle, 2011).

Constructivism does not say whether competition or cooperation is bound to happen; instead, it focuses on the social processes that lead to these outcomes (Onuf, 2002). It emphasizes the power of language and speech acts in creating meaning and establishing social rules that guide behavior, thereby building our reality. While identities shaped by society can change through back-and-forth interactions, they can also become deeply rooted within states and societies, often taking a long time to shift (Palan, 2000). This perspective suggests that by understanding identities as social constructs influenced by words and interactions, policymakers have more options to shape domestic and international relations.

Techno-authoritarianism

Techno-authoritarianism describes how a state uses information technology to control or manipulate people, both within its own borders and in other countries. This includes widespread surveillance, like facial recognition, internet censorship, cutting off internet access, spreading false information, and digital social credit systems (Drexel, 2025). The foundation of this model, particularly manifest in China, is an advanced, widespread, and often real-time surveillance system that combines government and private sector data. This organized sharing of data gives governments large access to information, which they then use to analyze and influence behavior through algorithms based on the regime's rules (Hillman, 2021).

This system develops a society where integration in the economy and daily life is based upon a "good credit rating" (Bernot et al., 2022). Those who are not in accordance with regulations are subject to penalties that have a marked effect upon their status. While a few are content to link this trend to dictator governments, digital methods of authoritarianism are equally in place in authoritarian and self-proclaimed democratic governments (Cave et al., 2019). This trend is a matter of concern globally as technologies can be developed to increase efficiency or as a defense serving to maintain governmental authority and oppress opposition.

Table 1

Differences of Selected Theories and Perspectives regarding State Power and Security

	Panopticism	**Securitization Theory**	**Constructivism**	**Techno-authoritarianism**
Nature of Power	Pervasive, internalized, psychological control through constant visibility	Discursive, achieved through "speech acts" framing issues as existential threats	Socially constructed through shared ideas, identities, and interactions	Centralized, technologically-enabled control and manipulation of populations
Origin of Threat	Internalized gaze, self-regulation due to potential observation	Not objective; constructed by actors to legitimize extraordinary means	Not inherent; threats are given meaning through social interaction and shared understandings	State-defined threats to regime stability, often framed as security or social order
Role of Technology	Mechanism for pervasive, psychological surveillance and control	Tool for implementing "extraordinary means" once an issue is securitized	Influences the social construction of identities and norms, but its impact is shaped by social choices	Core instrument for mass surveillance, censorship, and behavioral control
Focus	Micro-level control, individual self-discipline, architectural design as power	Macro-level political process, framing of issues, legitimization of emergency measures	Intersubjective meanings, identities, norms, and their evolution in international relations	State control over populations through digital means, social credit systems

Dual-use technologies and ethical dilemmas

Many technologies, from advanced computers to biological research, have a dual-use nature (Fischer, 2006) and can actually have legitimate civilian uses. However, such dual-use technologies can also be utilized to meet either military or perilous needs (Wallerstein, 1991). This duality in itself raises great ethical and regulative concerns in international relations. Dual-use goes beyond civilian or military intentions (Carrillo, 2017); it also includes research that might have misuse for illicit weapons programs, crime, or terrorism.

There is always a conflict between efforts to restrain the spread of dangerous capabilities and the requirements for international cooperation in sharing

technology (Fuhrmann, 2008). Treaties try to impede the spread of dangerous tools and also enable the peaceful transfer of technology (Boyer et al., 1996). The subjective element of intended use makes regulation even harder, as global enforcement is difficult to be achieved without strong administrative procedures. This can lead to a conceptual imbalance in how the world is governed, where the economic benefits of producing dual-use items (like making things cheaper by producing them in large quantities) can clash with security risks or ethical concerns when these technologies are sold to potentially untrustworthy actors (Nelson et al., 2022). For instance, a biotech breakthrough designed for public health could be repurposed for biological warfare (Evans, 2013), or an AI system (Kania, 2018) for autonomous driving might be adapted for weaponized drones.

Dual-use technologies also challenge fundamental principles of international humanitarian law (UN, 1949; UN, 1977a; UN, 1977b; UN, 1954; UNESCO, 1999; UN;1972; UNODA, 1980; UN, 1993; UN, 1997; UN, 2000) , such as the principle of distinction (UN, 1977a; Article 48, 51(2), 52(2)), which requires clear separation between civilian[2] and military targets in warfare, and the principle of proportionality (UN, 1977a; Article 51(5)(b), 57), which prohibits attacks causing excessive civilian harm relative to military advantage.

From a legal standpoint, there exists a persistent tension between efforts to prevent the proliferation of dangerous capabilities and the desire to foster international technological cooperation. International treaties aim to prevent the spread of dangerous tools[3] (UN, 1968; UN, 1972; UN, 1976; UNODA, 1980; UN, 1993; UN, 1996; UN, 1997; UN, 2008; UN, 2013; UN, 2017) while promoting peaceful technological exchange. The subjective element of intended use (UN, 1977a; Articles 50-56) makes global enforcement difficult without robust administrative procedures. This can lead to a conceptual imbalance in global governance, where economic benefits, such as those derived from mass production, can conflict with security risks or ethical concerns is these technologies are transferred to potentially untrustworthy actors (Gallagher et al., 2023).

To address these challenges, the European Union (EU), for example, has established a regulatory framework (Regulation 2021/821). However, regulatory inconsistencies across borders and the rapid evolution of emerging technologies like AI, biotechnology, and quantum computing pose ongoing hurdles. Therefore, research collaborations should undergo human rights assessments to prevent contributing to or profiting from human rights violations, and policies should uphold human rights and ethical principles, possibly using a human-rights-by-design approach (Penney et al., 2018).

Public opinion and state legitimation

States adopt innovative technological advancements in an attempt to advance their agendas since they need to rationalize their actions in a bid to remain legitimate globally and locally. This position in its subject presents a quandary of how to achieve a consensus in popular opinions, a situation that compels governments to adopt measures in determining political agendas. According to critical theory, leaders utilize media as a tool in building consensus among the masses. This is to make sure that public opinions are aligned with leaders' interests, underpinning their legitimacy and control over different political as well as economic institutions (Fuchs, 2016). Moreover, this mandate of authority is usually supplemented by a sequence of formalized procedures aimed at filtering and managing information, which affects not only the type of information available to populations but also how information is interpreted.

Manufacturing consent and the public sphere

The theoretical model of the public sphere, constructed by Jürgen Habermas, is one of the foundational pillars underpinning modern digital transformation. He (1991) theorizes that the public sphere refers to a particular social space in which individual members of the public come together to discourse, thus becoming the site for the exercise of public reason and the creation of public opinion. It is, in effect, the aggregate group of private citizens becoming a single entity to voice society's demands vis-à-vis the state (Habermas et al., 1974). The underlying foundations include logical and analytical thinking, readiness to be available, and bringing forth communicative power to justify political participation (Fraser, 2018). Despite such values, the typical public sphere shows significant flaws. Those active within it have been mainly comprised of educated male property-owning members of the bourgeoisie (Mckeon, 2004).

The idea of access guaranteed to all citizens is more an ideal than a reality that has ever been fully achieved in its original conception (Asen & Brouwer, 2001). This dual nature creates a more realistic benchmark for assessing the democratizing potential of virtual worlds (Adut, 2012). In addition, Habermas (1991) asserted that this sphere itself was eventually destroyed by the same forces that initially created it. This argument seems to uncover an intrinsic vulnerability, insinuating that together with the capitalist economic framework, institutions of the state, which made its establishment possible, simultaneously led to its decay. Such decay took place in tandem with marketization processes and indistinction between private and public spheres (Finlayson, 2019).

Herman & Chomsky's manufacturing consent theory (1988) argues that mass media is not a neutral space for different ideas. Instead, it acts as a powerful tool for powerful groups to maintain control over political and economic systems. It forms a public opinion that represents the interests of the powerful, and generally to the detriment of the masses. The theory states that information and news are filtered through a variety of structural filters. These include control of the media by interest-driven corporations with heavy capital and vested interests, reliance on advertising revenue and on state sources (Jackson & Stanfield, 2004), use of flak against critical voices, and perpetuation of master ideologies even through virtual media (Fuchs, 2018).

In this vein, media can contribute to a democratic deficit through the production of a passive audience and the acceptance of narratives without analyzing them (Müller, 2016), thus limiting the ability of citizens to hold power to account. The contribution of the media in shaping public opinion is vast, as it constructs images of the world beyond their reach on which citizens rely.

Public opinion formation and state legitimacy

In a democratic government, citizens play a central role as voters who choose representatives to make major choices and policies aligning with their priorities and beliefs. It compels citizens to engage actively in political processes, seek out contemporary information, develop opinions, and make independent, informed decisions based on values.

Walter Lippmann (1922), one of the critics of mass democracy, provided a negative assessment of the general public. He contended that common citizens, at best, have access to factual information or genuine concern for such information insufficiently. According to him, the information they can access is highly biased by individual propensities and the influences of mass communications. He proposed that people develop a pseudo-environment (Coffey, 1974), a subjective and truncated mental map of reality. While his assessment addressed mass media, it has some implication for today’s social media world as well. John Dewey (2012) while also acknowledging that citizens are imperfect, was more hopeful. He emphasized the potential to strengthen the public and saw public opinion as the best safeguard for democracy. For Dewey, a state's legitimacy is tied to its ability to organize the public for collective action and to serve the public's interests, especially in balancing individual actions that have indirect, far-reaching consequences.

A state's ability to make its actions seem legitimate, especially when new technologies are involved, depends on how it frames issues and manages public perception. When citizens are exceedingly uninformed about political matters, as some research suggests (McMurray, 2015; Markowski, 2020; Silver et al., 2024; Boudreau, 2009), they might rely on simple stories or cues, making them vulnerable to manipulated information. This highlights how important it is for states to control information and shape narratives to maintain their legitimacy, particularly when controversial technologies or policies are involved.

The evolving digital public sphere

The traditional public sphere, defined by clear spatial and architectural delimitations, has lost relevance due to procedures linked to depoliticization (Barney, 2014) and commodification (Ziółkowski, 2004). Equally, the virtual public sphere (Nanz, 2018), by its very nature linked to corporate platforms shaped by market forces and regulated by sophisticated algorithmic control, has similar, if not more severe, challenges concerning its autonomy and ability to deliberate. Such a historical process is vital to understanding difficulties within the digital public sphere (Enjolras & Steen-Johnsen, 2017).

Unlike prior theories of mass media, the world wide web spawns bifurcation and a public space (Ward, 1997). Social media encourages exposure to contrasting perspectives, shares information promptly, and supports bottom-up direct interaction without mainstream media as brokers (Hier, 2008). This could fortify action against official narratives of governments, ensuring accountability. However, there are challenges. Misinformation spreads quickly, echo chambers exist, and people are manipulated by complex algorithms (Sample et al., 2019). For governments, building trust is a challenge while dealing with diverging and inconsistent information.

Social media promotes the propagation of polarizing content, inducing political extremism and polarization in an urge to boost user engagement (Keene et al., 2017). This encourages echo chambers that destroy institutional trust, disdain facts, and diminish civic discourse, undermining democratic values.

Non-transparent algorithms are harmful and contribute to the aggravation of existing ills. The explosive spread of computerized content does not allow separating fact from lie, leading to informational pollution, which has a detrimental impact upon psychology at individual as well as social levels. This is a latent danger of digital authoritarianism, in which information as well as public opinion are manipulated in secret, and there are harsh consequences (Wright, 2019). Margetts

et al. (2016) address concerns that misinformation and extremist views cloud truth and falsehood, undermining democratic discourse.

The pluralistic public space of the internet could become polarized, privileging sensational narratives or algorithm bias over objective facts. Chaotic pluralism[4] is not likely to yield better deliberation. Rather, this development will intensify social fragmentation, move towards a loss of faith in the institutions of a democratic system, and diminish the capabilities for mass problem-solving. It, hence, represents a considerable danger for the integrity and efficacy of democratic regimes. The commercialization of the public space fundamentally changes the exercise of power in the virtual public space. When citizens are primarily consumers, whose information and attention are potential commodities for exploitation, the exercise of critical thinking by citizens, who should be self-determining agents and legitimate participants (Winston et al., 2023), encounters significant risk.

New dimensions: new technologies and justification strategies in the Israeli context

The case from Israel is a very strong example of practical application of the previously described abstract theoretical approach, which offers interesting insights into the dynamic process of how different states apply technologies and what their underlying motivations are. The territories of the Gaza Strip and the West Bank have been described by a variety of commentators as being akin to a virtual outdoor prison (Feldman, 2015). The technological products being tested in a first phase against the people in the Gaza Strip as well as in the West Bank are sold in a later phase, on a global basis, under the marketable description of being combat-proven or battle-tested in action (Action & Corbyn, 2024).

The total earnings from armaments deals by three Israeli companies[5] ranked in the Stockholm International Peace Research Institute (SIPRI)'s top 100 lists reached $13.6 billion by the end of 2023 (SIPRI, 2023), a historical high. In 2024, Israeli defense exports grew by 13 percent to about $14.7 billion, another record, having doubled in the last five years (Embassy of Israel Kathmandu, 2025). The global border security industry, currently worth over $65 billion, is expected to reach about $112 billion by 2030, and Israel is set to grab a big piece of this growing market (Research and Markets, 2025). This shows a unique model in which a long-standing conflict and occupation are directly used to power a booming defense industry, creating a self-sustaining economic reason to maintain certain policies.

The digital intelligence apparatus: unit 8200 and digital apartheid

At the heart of Israel's technological control is Unit 8200, the IDF's signal intelligence and cyber intelligence gathering unit, often called Israel's digital intelligence brain (Foreign Policy, 2007; Senor & Singer, 2009). Founded in 1952 (Jewish Voice Ministries International, 2018), this unit has been crucial in collecting vast amounts of data on Palestinians worldwide. It uses tools like wiretapping, internet surveillance, cyberattacks, AI, big data analysis, psychological pressure, blackmail, and social network mapping. Former Unit 8200 personnel have even admitted to using highly personal information, including sexual orientation, psychological trauma, and debts, for intelligence purposes (Cooper, 2014; Arab News, 2025).

A significant aspect of this system is the revolving door phenomenon. Many who leave Unit 8200 start their own cybersecurity companies, exporting technologies tested in the 'Palestinian laboratory' globally with state support (Loewenstein, 2023). Companies like the NSO Group (known for Pegasus spyware), Cellebrite, Paragon Solutions, Candiru, Quadream, Cytrox, Black Cube, and Intellexa were founded or managed by former Unit 8200 employees (European Parliament, 2023). This creates a direct link from state military intelligence to the private defense and surveillance industry, blurring the lines between government and corporate interests. This close relationship ensures that technologies developed under occupation find profitable global markets, effectively privatizing and globalizing the expertise gained from controlling a subjugated population.

Many technologies are used to control the Palestinian population, showing a system of widespread surveillance and siege. Gaza, for example, is surrounded by wire fences, drones, and listening devices (Shlaim, 2024), aiming to keep it as the world's largest open-air prison (Norwegian Refugee Council, 2018). In the West Bank, Palestinian movements are extensively recorded using facial recognition and biometric data, to automate control and minimize human interaction (Kilgore, 2022). Surveillance in Palestinian neighborhoods is notably higher than in mostly Jewish areas. According to the United Nations Office for the Coordination of Humanitarian Affairs (OCHA) (2025), there were 593 checkpoints in the West Bank in 2020 and 849 in 2025 that restrict Palestinian movement.

Specific technologies that have been utilized by Israel highlight the following:

- Mabat 2000: This advanced surveillance system in Jerusalem's Old City uses hundreds of networked cameras, intelligent video analysis, license plate recognition, and facial recognition. It is described as a tool of digital apartheid (Amnesty International, 2021) against Palestinians in East

Jerusalem. The system's goal is for Big Brother[6] to have complete control (Who Profits, 2018).

- Blue Wolf: An Israeli army facial recognition app used by soldiers in the West Bank. It allows instant scanning of Palestinian faces against a central database (Wolf Pack) to access personal data, security levels, family history, and detention information (Goodfriend, 2024). Soldiers are reportedly required to upload at least 50 Palestinian photos per guard duty, creating a competitive game, where soldiers are rewarded for collecting more data (Kubovich, 2022).
- Smart Shooter: An AI-powered remote crowd control platform used in Hebron. It deploys tear gas, sponge-headed bullets, and stun grenades, with target acquisition handled entirely by AI based on factors like criminal records, facial expressions, and body language (Mayfield & Roaten, 2021). This technology turns crowd control into a smart warfare product, allowing for automated, potentially deadly, decision-making without a human directly identifying a threat (Antebi & Yanko-Avikasis, 2023).
- Pegasus (NSO Group): This advanced spyware infects smartphones with access to microphones, cameras, GPS data, contacts, messages, and encrypted applications (Bamford, 2016). First used against Palestinian activists, journalists, and diplomats, it is then sold globally as battle-tested. Its ability to remain silent and undetected, even while collecting data, makes it a powerful tool for secret surveillance (Feldstein & Kot, 2023).
- Cellebrite: A forensic analysis system used at checkpoints to extract all data from physically accessed mobile phones, including encrypted or deleted content.[7] This allows soldiers to quickly download private messages, social media conversations, location data, and internet history (Shewring, 2025). Algorithms then analyze social circles, political views, and radical tendencies. This practice represents a deep invasion of privacy and a systematic data harvesting operation on an entire population (Simon & Mahoney, 2022).
- AnyVision (Oosto): This company installs facial recognition cameras at checkpoints and residential areas in the West Bank. It processes biometric data, facial expressions, clothing, and companions through AI analysis to constantly monitor and predict behavior. The system, reportedly applied only to Palestinians in the West Bank, shows a discriminatory use of surveillance technology (Abu-Sittah, 2020). The project, known as Google Ayosh (referring to the technology's "ability" to search for people and "Ayosh" for occupied Palestinian territories), even received Israel's top defense award (Dayan, 2022).[8]

Together, these examples show a system of digital apartheid, where unequal access to digital technologies and information makes existing inequalities even worse. Data from underserved populations is collected and sold, but rarely used to empower them; instead, surveillance takes priority over providing services. This creates a moral paradox,[9] where innovation is used to control and subjugate a people rather than serve humanity, raising concerns about the disconnect between advanced technology and the daily lives of those under surveillance.

Table 2

Convergence of Technologies and Justification Strategies in Practice

	Surveillance Technologies (Mabat 2000, Blue Wolf, AnyVision)	**Spyware (Pegasus, Predator)**	**Crowd Control/ Targeting (Smart Shooter, Drones)**	**Data Extraction (Cellebrite)**
Primary Application	Mass monitoring, facial recognition, movement tracking	Covert access to personal data, communications, location	Automated targeting, remote control, intelligence-driven force	Comprehensive data scraping from mobile devices
Justification Narrative	"Security," "preventing attacks," "saving lives"	"Combating worst actors," "fighting crime/terrorism"	"Combat-proven," "tactical superiority," "tested in war zones"	"Forensic analysis," "dismantling pedophile networks," "rescuing children"
"Battle-Tested" Context	Palestinian territories (West Bank, East Jerusalem)	Palestinian campaigners, journalists, diplomats	Gaza, Hebron	Palestinian checkpoints
Global Export/ Use	Widely exported, used in various countries	Sold to numerous countries	Exported to many countries	Sold to lots of countries, used by US state police
Impact on Civilians	Pervasive monitoring, digital apartheid, dehumanization	Invasion of privacy, targeting dissidents, journalists	Automated decision-making, potential for indiscriminate harm	Profound privacy invasion, systematic data harvesting, profiling

Justification Strategies and International Complicity

Israel uses specific strategies to justify its technological practices and exports. A main method is labeling technologies as combat-proven or battle-tested (JPS, 2015), using their deployment against Palestinians to suggest effectiveness and reliability. This marketing story positions Israel's defense industry as one of the global leaders.

Another key justification involves presenting these technologies as essential for security and saving lives (Rowland, 2016). Companies like Cellebrite promote their products as tools to dismantle pedophile networks and rescue abducted children (OFTA, 2025; PI, 2025), while NSO Group's CEO claims their technology fights against the criminals (Simons, 2025). This narrative tries to make the technologies seem legitimate by linking them to universally accepted moral goals, deflecting criticism about their use in human rights abuses. When facing international pressure, Israeli companies often use a similar narrative arguing that they enhance other countries' safety and security, which shifts the responsibility to the buying country (Zahra, 2023).[10]

Beyond marketing, Israel uses diplomatic channels and foreign policy to promote these exports. The Ministry of Defense licenses sales (Azulay, 2024), while Mossad or the Ministry of Foreign Affairs handles diplomatic aspects, allowing for strategic alliances without formal military relations (Berman & Staff, 2025). Mossad's involvement in secret negotiations for Pegasus with countries like Saudi Arabia (Jones, 2025), despite no official diplomatic ties, highlights how important these technology sales are as foreign policy tools. Agreements with African countries are even linked to efforts to influence votes at the United Nations General Assembly (Oded, 2010).

The global spread of these technologies is further enabled by what seems to be international complicity or ignorance by western democracies. US state police actively uses Cellebrite systems (Gelardi, 2022) and the UK uses NSO solutions through private security companies (Kirchgaessner et al., 2020). A particularly striking example is the EU's border guard agency, Frontex, which signed a €100 million contract with Israeli companies like Elbit Systems and Israel Aerospace Industries for drones to monitor migrants in the Mediterranean (European Parliament, 2020). These drones, also tested in Gaza, carry advanced equipment and can detect migrant boats, but offer no direct rescue capability, potentially allowing migrants to drown or be handed over to the Libyan Coast Guard (Euro-Med Human Rights Monitor, 2020). This suggests a boomerang effect, where

repressive tools and practices, perfected in one setting, are then applied elsewhere, eroding civil liberties and democratic norms globally.

Furthermore, the European Space Agency (ESA), a publicly funded institution, has built commercial networks with Israeli arms companies, including Elbit, for projects like the Venus mission and the Copernicus Earth observation satellite program (Cronin, 2025). This collaboration, even though Elbit[11] is banned from some international fairs, shows how commercial interests and perceived technological advancement can override ethical concerns and international pressure. The ability of an Elbit subsidiary, OIP Space Instruments- OIP nv (Optronic Instruments and Products) (VRI, 2025), to participate in a contract rivalry (OIP, 2025a) presenting itself as a Belgian company (OIP, 2025b), despite the ban on Israeli arms manufacturers (Martinez, 2025), further demonstrates the clever methods used to get around restrictions and normalize these technologies.

The Role of Censorship, Narrative Control and Global Surveillance

A crucial element supporting the Palestine Laboratory is censorship and control over the narrative. Social media companies like YouTube, Facebook, Instagram, TikTok, and X (previously Twitter) regularly block content that criticizes Israel or presents Palestinian viewpoints (Shankar et al., 2023). Palestinian posts containing words like "resistance" or "martyr" are automatically flagged by algorithms as "incitement to violence" and removed, while Israeli posts with racist language often bypass these filters (Lewis, 2021).

This suggests a form of platform complicity in state-sponsored narrative control. Big tech companies which have social platforms such as YouTube, X, TikTok, Facebook and Instagram have removed tons of content at Israel's request through Iron Truth, Digital Dome and Fake Off projects[12] (Biddle, 2024). This privatized censorship, carried out by algorithms on global private social media platforms, effectively extends the reach of state propaganda and suppresses dissent far beyond national borders. It raises serious questions about the power of tech companies as gatekeepers of global discussion and their responsibility to human rights and ethical principles.[13] The systematic suppression of one narrative while allowing another, even if it contains hate speech, creates an uneven playing field in public discourse, making it difficult for a truly informed public opinion to form and for the state's actions to be critically examined.

Beyond the Israeli context, the world is increasingly observing companies and states using similar surveillance and control technologies, often with concerning human rights implications. A prime example of digital authoritarianism, China has

developed and exported its model of state-controlled internet namely Great Firewall (Tkacheva et al., 2013) and widespread surveillance systems. Companies like Hikvision, ZTE, Huawei and Dahua the world's largest maker of surveillance equipment (Groot, 2020), and AI startups such as Claudwalk, SenseTime, Yitu, and Megvii, are central to China's vast surveillance network, which includes millions of CCTV cameras and facial recognition (Khalil, 2020; Byler, 2022). China has sold surveillance and monitoring systems to many countries, serving as a blueprint for other regimes (Feldstein, 2019; Kang & Grauer, 2025).

Russia's approach to digital authoritarianism involves strict laws on online expression and technologies to enforce them, including surveillance of all internet traffic through systems like SORM and the Semantic Archive. Russian companies also export surveillance and hacking technologies, especially to former Soviet states, contributing to the suppression of dissent (Morgus, 2019).

Iran has adopted digital surveillance methods, although it is not accepted as a mass surveillance tactic against all of the population. But it includes deep packet inspection and targeted surveillance, as part of its strategy of political repression, often targeting human rights activists and journalists (UK Government, 2025).

The global video surveillance market, valued almost at $237 billion, includes major players such as Bosch Sicherheitssysteme GmbH (Robert Bosch GmbH), Axis Communications AB (Canon Inc.), Eagle Eye Networks Inc., Honeywell International Inc., Hangzhou Hikvision Digital Technology Company Limited, Infinova Corporation, Qognify Inc., Panasonic Corporation, Schneider Electric SE, Sony Group Corporation, Samsung Electronics Co. Ltd., Zhejiang Dahua Technology Co. Ltd., Qognify Inc., and Samsung Electronics Co. Ltd. They also deal in a variety of products such as network cameras, video management software, and analysis software, which can be utilized in different applications such as security, traffic management, and safety of valuable infrastructure (IMARC, 2025).

Exportation of cyber-surveillance equipment by many states raises serious concerns about human rights because such equipment is often used for political opposition, journalists, and human rights advocates (Lyon, 2019). While a few states have made commitments to enact export controls and due diligence standards (EU, 2024), the prevalence of the states lacks such controls and allows for unrestricted business by manufacturers. This highlights the need for a global agreement to prevent the spread of technologies that enable serious human rights abuses.

Conclusion

The surveillance process entails several actors functioning within a securitization framework consisting of government institutions, national security systems, and information technologies sectors, which are increasingly privately owned. The involvement of these actors at various instances harbor inevitable dangers. The implementation of new-age technology and the enhancement of high-tech projects highlight fundamental aspects of the transformation of international relations and social structures in the 21st century.

This research ultimately demonstrates that technology operates as both a mechanism of governance and a commodity of power. The theoretical frameworks introduced in the beginning—particularly panopticism, securitization theory, constructivism, and techno-authoritarianism—collectively illuminate how surveillance systems transform from instruments of control into tradable goods with strategic and symbolic value. In this sense, technology becomes not merely a means of maintaining order, but an exportable asset that reinforces the authority and legitimacy of the state in domestic and international arenas alike.

The Palestine case unveils how occupation and conflict spur economic advancement and industrialization. The latter is promoted by Israeli war exports, which are hailed as effective products. Efficacy legitimizes the marketing of war exports, which encourages the economy but could also fortify conflict as beliefs concerning potential risks are refuted.

State intelligence units, such as Unit 8200, are inextricably connected to the newly emerging private information-security market, forming an active governance entity. The new trend of individuals swapping roles between intelligence activities in the army and establishing different global technology companies ensures that research and development, initially planned for domestic governance, are quickly and effectively converted into commercial enterprises. Then, these become disseminated internationally. The smooth convergence between commercial and army interests obfuscates boundaries, traditionally distinguishing between public and private spheres, and opens a variety of thorny and pressing questions concerning accountability, regulatory mechanisms, as well as ethical repercussions, connected to the current trend of privatization of state surveillance mechanisms.

The Israeli case embodies this dual transformation vividly. Surveillance and military technologies developed under conditions of occupation are repackaged as “combat-proven” innovations and sold globally, creating a self-sustaining cycle

where conflict and control feed economic growth. The global demand for such technologies reveals how narratives of security, humanitarian necessity, and innovation merge to justify practices that would otherwise raise ethical concern. Thus, the empirical findings reinforce the theoretical claim that technology, once commodified, becomes a diplomatic and economic instrument that extends a state's influence beyond its borders.

It is pertinent to note that such extensive use of most advanced and state-of-the-art spying technologies, such as Mabat 2000, Blue Wolf, Smart Shooter, Pegasus, Cellebrite, and AnyVision, in the territories of the West Bank and the Gaza Strip amounts to what one may call a highly advanced digital apartheid.

These technologies are not being designed solely for purposes connected to security; instead, they are specifically meant for exerting control, dehumanizing people, and practicing systematic discrimination against entire populations. The final objective in this case is to facilitate the automation of oppression and increase the current occupation of these territories at a larger scale. Further, incorporation of gamification methods in order to facilitate efficient tracking of targeted people, employment of artificial intelligence in facilitating pinpoint targeting, and the indiscriminate and wholesale data collection from the entire citizenry indicate a comprehensive and alarming erosion of constitutional rights such as the right to privacy and human dignity.

Israel is trying to legitimize its actions through western democracies and international social media. This is a concerning validation of repressive action and technology, commonly justified as a need in national security issues, though used in countries where human rights are not upheld. The boomerang effect emerges when such war-zone technology is adopted by democratic governments and used indiscriminately at borders, violating civil liberties. Furthermore, social media facilitates constraining criticism on Israel, where counterfactual narratives are in abundance. This poses a worrying trend of normalizing control over narratives and challenges democratic discourse. Thus, the Israeli case study illustrates how technological developments converge on geopolitical situations and state requirements. In our current age of information, this dynamic consolidates control over frontiers in contravention of international rules and shifts power dynamics among states.

Notes

[1] Another term "Automated Apartheid" is used by Amnesty International for a limited apartheid structure (Amnesty International, 2023). In this study, however, digital apartheid is intentionally used to emphasize the scope the apartheid.

[2] An investigation by The Guardian, Local Call and +972 Magazine shows that only 1 in 4, quarter, Palestinians captured by Israel defined as militant (Abraham, 2025).

[3] In addition to the treaties, pleas also see: 1987 Missile Technology Control Regime (MTCR) (2017); The Hague Code of Conduct against Ballistic Missile Proliferation (HCOC) (2002); UNSC Resolution 1540 (2004); Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons (UNSGM) (UNSC Resolution 620 (1988)); Measures to Prevent Terrorists from Acquiring Weapons of Mass Destruction (UNGA, 2002); Mine Action and Effective Coordination: the United Nations Inter-Agency Policy (UN, 2005); UN Mine Action Service (UNMAS) (UN, 2025a); UN Safeguard Programme (UN, 2025b); Women, Disarmament, Non-proliferation and Arms Control (UNGA, 2010); Youth, Disarmament and Non-Proliferation (UNGA, 2023).

[4] Chaotic pluralism defends the idea that individuals can make some contributions to the political system via social media, leading to large-scale mobilization. In contrast, classical pluralism rejects monastic conception of the state or politics through bigger groups in the system. It is a system to constrain the absolute power with the plural power system. For the classical pluralism please see: Dahl (1961; 1978), Lukes (1974), Lindblom (1983).

[5] Elbit Systems, Israel Aerospace Industries, Rafael. Details for Elbit Systems and partner countries, see the research center report (Who Profits, 2025).

[6] A state that tries to control everything through the surveillance of the population. For details, see (Beauchamp, 1984; Galantonu, 2016).

[7] In a recent official declaration, PM Netanyahu remarked "… You have cell phones here? … You're holding a piece of Israel right there…" (Prime Minister's Office, 2025).

[8] In addition to these companies, Palantir is also worthy to be mentioned with its two subdivisions namely Gotham and Foundry. But these platforms are capable beyond surveillance. They are directly integrated with the governments and play a decision-making role in official entities. So, they may create severe consequences for the public apart from expected progress. For details, see (Bennett, 2025); (Joh, 2025), (The American Immigration Council, 2025), (Fürstenau, 2025).

[9] Political repression may even prevent the literature or poems from being independent (Steiner, 1986).

[10] Even Israel itself is controlling the narrative through exchanges of statements between English and Hebrew (Lindley, 2025).

[11] Elbit is the most significant Israeli government company which was also rewarded recently. For more details, see the report by The Office of the United Nations High Commissioner for Human Rights (OHCHR, 2025).

[12] For an Israeli explanation about the necessity of the projects, see (Yasur & Ring, 2024).

[13] For EU warnings about these companies, see (Business & Human Rights Resource Centre, 2023a, 2023b, 2023c, 2023d)

Article Information Form

Conflict of Interest: Authors have no conflict of interest to declared.

Support/Supporting Organizations: No grant was received from any public institution, private or non-profit sector for this research. (If there is a supporting organization, the authors should indicate this).

Artificial Intelligence Statement: No artificial intelligence tools were used while writing this article.

Plagiarism Statement: This article was scanned by iThenticate.

References

AA. (2025, May 15). Interview – 'Expose them': Viral Palantir protester warns all complicit in Gaza horrors. https://www.aa.com.tr/en/middle-east/interview-expose-them-viral-palantir-protester-warns-all-complicit-in-gaza-horrors/3565328

Abraham, Y. (2025). Israeli intelligence data: Militants account for only 1 in 4 Gaza detainees. *+972 Magazine*. https://www.972mag.com/israeli-intelligence-database-militants-civilians-gaza-detainees/

Abu-Sittah, G. (2020). The Virus, the Settler, and the Siege: Gaza in the Age of Corona. *Journal of Palestine Studies*, *49*(4(196)), 65–76.

Action, P., & Corbyn, J. (2024). Direct Action against the Arms Trade. In R. Michie, A. Feinstein, & P. Rogers (Eds.), *Monstrous Anger of the Guns: How the Global Arms Trade is Ruining the World and What We Can Do About It* (1st ed., pp. 164–171). Pluto Press.

Adut, A. (2012). A Theory of the Public Sphere. *Sociological Theory*, *30*(4), 238–262.

Amnesty International. (2021). Stop the automated apartheid in Palestine. https://www.amnesty.org/en/petition/stop-the-automated-apartheid-in-palestine/

Amnesty International. (2023). Israel and Occupied Palestinian Territories: Automated Apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT. https://www.amnesty.org/en/documents/mde15/6701/2023/en/

Antebi, L., & Yanko-Avikasis, M. (2023). *Life and Death in the Hands of the Drone: The Small, Cheap Devices Early in the Swords of Iron War*. Institute for National Security Studies.

Arab News. (2025). Israel's Unit 8200 used Microsoft cloud to store 'a million calls an hour' of Palestinian phone conversations. https://www.arabnews.com/node/2610908/world

Asen R. and Brouwer D. C. (2001). Introduction: Reconfigurations of the Public Sphere. In Asen R. and Brouwer D. C. (eds), *Counterpublics and the State*. Albany, State University of New York Press.

Azizian, A. (2022, July 28). Iran crude/condensate review H1 2022. *Vortexa*. https://www.vortexa.com/insights/crude/iran-crude-condensate-

review-h1-2022/?utm_source=marketo&utm_medium=email&utm_campaign=insights210722&mkt_tok=ODM3LU1aRS01NzgAAAGFwGyFMoSJPii_0tozPvKU4hVvpfYcYqGygOQSZPTG5abBNmT0xvLdA-78arosRGTraIqkG9bL4Z8_Czt116Pei7DQmpMhs6ymajvJWW0

Azulay, Y. (2024). Israel to ease defense export rules, opening local market to new international buyers. *Ynet Global*. https://www.ynetnews.com/business/article/ryba4b37kl

Baldwin, D. A. (2016). Constructivism. In *Power and International Relations: A Conceptual Approach* (pp. 139–154). Princeton University Press.

Bamford, J. (2016). national security: The Espionage Economy. *Foreign Policy*, *216*, 70–72.

Barney, D. (2014). Publics without Politics: Surplus Publicity as Depoliticization. In K. Kozolanka (Ed.), *Publicity and the Canadian State: Critical Communications Perspectives* (pp. 70–86). University of Toronto Press.

Beauchamp, G. (1984). Big Brother in America. *Social Theory and Practice*, *10*(3), 247–260.

Bennett, N.M. (2025). *When the government can see everything: How one company – Palantir – is mapping the nation's data.* The Conversation. https://theconversation.com/when-the-government-can-see-everything-how-one-company-palantir-is-mapping-the-nations-data-263178

Bentham, J. (1843). Principles of Penal Law. In J. Bowring (Ed.), The Works of Jeremy Bentham Vol. 4, Edinburgh: William Tait.

Berman, L. and Staff, T. (2025). Report: Netanyahu approved major deals between top Israeli defense companies and Qatar. *Times of Israel*. https://www.timesofisrael.com/report-netanyahu-approved-major-deals-between-top-israeli-defense-companies-and-qatar/

Bernot, A., Trevaskes, S., & Strange, S. (2022). Smart Governance, Smarter Surveillance. In L. Jaivin & E. S. Klein (Eds.), *Contradiction* (1st ed., pp. 15–31). ANU Press.

Biddle, S. (2024). Israeli Group Claims It's Working With Big Tech Insiders to Cencor "Inflammatory" Wartime Content. The Intercept. https://theintercept.com/2024/01/10/israel-disinformation-social-media-iron-truth/

Boudreau, C. (2009). Closing the Gap: When Do Cues Eliminate Differences between Sophisticated and Unsophisticated Citizens? *The Journal of Politics*, *71*(3), 964–976.

Boyer, Y., Carle, C., Müller, H., & Van Orden, G. (1996). The Proliferation of Conventional Arms And Dual-Use Technologies. In J. Krause, P. Cornish, & P. van Ham (Eds.), *Europe And The Challenge of Proliferation*. European Union Institute for Security Studies (EUISS).

Business & Human Rights Resource Centre. (2023a). EU sends formal information request to Meta, TikTok over disinformation on Israel-Hamas war. https://www.business-humanrights.org/en/latest-news/eu-sends-formal-information-request-to-meta-tiktok-over-disinformation-on-israel-hamas-war/

Business & Human Rights Resource Centre. (2023b). EU digital chief urges TikTok & X Corp to increase efforts to remove harmful content on their platforms. https://www.business-humanrights.org/en/latest-news/eu-digital-chief-urges-tiktok-x-corp-to-increase-efforts-to-remove-harmful-content-on-their-platforms/

Business & Human Rights Resource Centre. (2023c). EU warns Google & YouTube over Hamas-Israel disinformation. https://www.business-humanrights.org/en/latest-news/eu-warns-google-youtube-over-hamas-israel-disinformation/

Business & Human Rights Resource Centre. (2023d). Access Now, Article19 & 28 CSOs urge EU to respect rule of law when tackling content about Gaza & Israel. https://www.business-humanrights.org/en/latest-news/access-now-article19-28-csos-urge-eu-to-respect-rule-of-law-when-tackling-content-about-gaza-israel/

Buzan, B. G., Wæver, O., & de Wilde, J. H. (1998). *Security: A New Framework for Analysis*. Lynne Rienner.

Buzan, B., & Wæver, O. (2009). Macrosecuritisation and Security Constellations: Reconsidering Scale in Securitisation Theory. *Review of International Studies*, *35*(2), 253–276.

Byler, D. (2022). Surveillance, data police, and digital enclosure in Xinjiang's 'Safe Cities.' In D. Byler, I. Franceschini, & N. Loubere (Eds.), *Xinjiang Year Zero* (1st ed., pp. 183–204). ANU Press.

Carrillo, P. E. (2017). *Commercial Dual-Use Technologies in Defense Acquisition Reform*. R Street Institute.

Castells, M. (2008). The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance. *The Annals of the American Academy of Political and Social Science*, *616*, 78–93.

Cave, D., Hoffman, S., Joske, A., Ryan, F., & Thomas, E. (2019). Enabling & exporting digital authoritarianism. In *Mapping China's technology giants* (pp. 08–15). Australian Strategic Policy Institute.

Coffey, J. W. (1974). The Five Faces of Walter Lippmann [Review of *Five Public Philosophies of Walter Lippmann.*, by B. F. Wright]. *Reviews in American History*, *2*(4), 546–552.

Cooper, H. (2014). Israeli soldiers from elite wire-tapping unit refuse to use 'extortion', 'blackmail' on Palestinians*. ABC*. https://www.abc.net.au/news/2014-09-13/israeli-soldiers-refuse-to-spy-on-palestinians/5741492

Cronin, D. (2025). *Space agency heads to Venus with help from genocide profiteer*. The Electronic Intifada. https://electronicintifada.net/blogs/david-cronin/space-agency-heads-venus-help-genocide-profiteer

Dahl, R. A. (1961). *Who governs?: Democracy and power in an American city*. Yale University Press.

Dahl, R. A. (1978). Pluralism Revisited. *Comparative Politics*, *10*(2), 191–203.

Dayan, H. (2022). Israel/Palestine: Authoritarian Practices in the Context of a Dual State Crisis. In Ö. E. Topak, M. Mekouar, & F. Cavatorta (Eds.), *New Authoritarian Practices in the Middle East and North Africa* (pp. 131–151). Edinburgh University Press.

Dewey, J. (2012). *The Public and Its Problems: An Essay in Political Inquiry* (M. L. Rogers, Ed.). Penn State University Press.

Drexel, B. (2025). *Promethean Rivalry: The World-Altering Stakes of Sino-American AI Competition*. Center for a New American Security.

Embassy of Israel Kathmandu. (2025). *Israel Ministry of Defense Spokesperson: Israel Sets New Record in Defense Exports: Over $14.7 Billion in 2024.* https://new.embassies.gov.il/nepal/en/news/israel-ministry-defense-spokesperson-israel-sets-new-record-defense-exports-over-147-billion#:~:text=Israel%20MOD%20announces%20that%20Israel's,increase%20over%20the%20previous%20year.

Enjolras, B., & Steen-Johnsen, K. (2017). The Digital Transformation of the Political Public Sphere: a Sociological Perspective. In K. Steen-Johnsen, F. Engelstad, H. Larsen, J. Rogstad, D. Polkowska, A. S. Dauber-Griffin, & A. Leverton (Eds.), *Institutional Change in the Public Sphere: Views on the Nordic Model* (1st ed., pp. 99–117). De Gruyter.

EU. (2021). Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast). https://eur-lex.europa.eu/eli/reg/2021/821/oj/eng

EU. (2024). Commission Recommendation (EU) 2024/2659 of 11 October 2024 on guidelines on the export of cyber-surveillance items under Article 5 of Regulation (EU) 2021/821 of the European Parliament and of the Council. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402659

Euro-Med Human Rights Monitor. (2020). EU Should Cancel €59M Contract with Israeli Companies for Drones to Surveille Migrants. https://euromedmonitor.org/en/article/3529/EU-Should-Cancel-€59M-Contract-with-Israeli-Companies-for-Drones-to-Surveille-Migrants

European Parliament. (2020). Procurement of Israeli drones for the surveillance of migrants in the Mediterranean. https://www.europarl.europa.eu/doceo/document/E-9-2020-003321_EN.html#def1

European Parliament. (2023). *Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware.* https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html

Evans, N. G. (2013). Contrasting Dual-Use Issues in Biology and Nuclear Science. In B. Rappert & M. J. Selgelid (Eds.), *On the Dual Uses of Science and Ethics: Principles, Practices, and Prospects* (pp. 255–274). ANU Press.

Feldstein, S., & Kot, B. (2023). Introduction. In *Why Does the Global Spyware Industry Continue to Thrive?: Trends, Explanations, and Responses* (pp. 5–6). Carnegie Endowment for International Peace.

Feldman, I. (2015). Gaza as an Open-Air Prison. *Middle East Report*, *275*, 12–14.

Feldstein, S. (2019). The Global Expansion of AI Surveillance. The Global Expansion of AI Surveillance. https://carnegie-production-

assets.s3.amazonaws.com/static/files/files__WP-Feldstein-AISurveillance_final1.pdf

Finlayson, J. G. (2019). *The Habermas-Rawls Debate*. Columbia University Press.

Fischer, J. E. (2006). Defining Dual-Use Technologies. In *Stewardship or Censorship?: Balancing Biosecurity, The Public's Health, and The Benefits of Scientific Openness* (pp. 43–45). Stimson Center.

Foreign Policy. (2007). Net Effect: How Technology Shapes the World. *162*, 92–93.

Foreign Policy. (2013). The Surveillance State and Its Discontents. *203*, 64–74.

Foucault, M. (2008). "Panopticism" from "Discipline & Punish: The Birth of the Prison." *Race/Ethnicity: Multidisciplinary Global Contexts*, *2*(1), 1–12.

Fraser, N. (2018). The Theory of the Public Sphere: The Structural Transformation of the Public Sphere (1962). In H. Brunkhorst, R. Kreide, & C. Lafont (Eds.), *The Habermas Handbook* (pp. 245–255). Columbia University Press.

Fuhrmann, M. (2008). Exporting Mass Destruction? The Determinants of Dual-Use Trade. *Journal of Peace Research*, *45*(5), 633–652.

Fuchs, C. (2016). Beyond Habermas: Rethinking Critical Theories of Communication. In *Critical Theory of Communication: New Readings of Lukács, Adorno, Marcuse, Honneth and Habermas in the Age of the Internet* (Vol. 1, pp. 177–206). University of Westminster Press.

Fuchs, C. (2018). Propaganda 2.0: Herman and Chomsky's Propaganda Model in the Age of the Internet, Big Data and Social Media. In J. Pedro-Carañana, D. Broudy, & J. Klaehn (Eds.), *The Propaganda Model Today: Filtering Perception and Awareness* (Vol. 8, pp. 71–92). University of Westminster Press.

Fürstenau, M. (2025). German police expands use of Palantir surveillance software. *Deutsche Welle*. https://www.dw.com/en/german-police-expands-use-of-palantir-surveillance-software/a-73497117

Gad, U. P., & Petersen, K. L. (2011). Concepts of politics in securitization studies. *Security Dialogue*, *42*(4/5), 315–328.

Galantonu, D. (2016). The Big Brother Fear: Four Perspectives on Surveillance. *American Intelligence Journal*, *33*(1), 59–64.

Gallagher, N. W., Rand, L., Entrikin, D., & Aoki, N. (2023). Post-Cold War controls on WMD-related technologies. In *The Desirability and Feasibility of Strategic Trade*

Controls on Emerging Technologies (pp. 33–49). Center for International & Security Studies, U. Maryland.

Gelardi, C. (2022). The State Police Want to Crack Your Phone. New York Focus. https://nysfocus.com/2022/11/23/new-york-state-police-phone-surveillance-cellebrite

Gouck, J. (2018). The Viewer Society: 'New Panopticism', Surveillance, and The Body in Dave Eggers' *The Circle*. *IJAS Online*, *7*, 57–64.

Goodfriend, S. (2024). Algorithmic Dissent: Militarized Platforms and Palestinian Political Imagination in Jerusalem. *Journal of Palestine Studies*, *53*(3), 36–53.

Groot, G. (2020). Schemes, Dreams, and Nightmares: China's Paradox(Es) Of Trust. In J. Golley, L. Jaivin, B. Hillman, & S. Strange (Eds.), *China Dreams* (pp. 198–212). ANU Press.

Habermas, J., Lennox, S., & Lennox, F. (1974). The Public Sphere: An Encyclopedia Article (1964). *New German Critique*, *3*, 49–55.

Habermas, J. (1991). *The Structural Transformation of the Public Sphere An Inquiry into a Category of Bourgeois Society*. The MIT Press.

Herman, E. S., & Chomsky, N. (1988). *Manufacturing consent: the political economy of the mass media.* Pantheon Books.

Hillman, J. E. (2021). *"Techno-Authoritarianism: Platform for Repression in China and Abroad."* Center for Strategic and International Studies (CSIS).

Hopf, T. (1998). The Promise of Constructivism in International Relations Theory. *International Security*, *23*(1), 171–200.

IMARC. (2025). Global Video Surveillance Systems Market to Reach USD 236.9 Billion by 2033, Propelled by Growing Incidences of Theft. https://www.imarcgroup.com/global-video-surveillance-systems-market

Jackson, P. T. & Stanfield, J. R. (2004). The Role of the Press in a Democracy: Heterodox Economics and the Propaganda Model. *Journal of Economic Issues*, *38*(2), 475–482.

Jewish Voice Ministries International. (2018). Israel's Unit 8200 Takes on Global Terrorism. https://www.jewishvoice.org/read/blog/israels-unit-8200-takes-global-terrorism

Joh, E. E. (2025). Police Technology Experiments. *Columbia Law Review*, *125*(1), 1–28.

Jones, M. O. (2025). Lessons from the Digital Coalface in the Post-Truth Age: Researching the Middle East Amid Authenticity Vacuums, Transnational Repression & Disinformation. *Daedalus*, *154*(2), 132–156.

JPS. (2015). Selections from the Press. *Journal of Palestine Studies*, *45*(1 (177)), 110–135.

Kang D., Grauer, Y. (2025). Silicon Valley enabled brutal mass detention and surveillance in China, internal documents show. *The Associated Press*. https://www.ap.org/news-highlights/spotlights/2025/silicon-valley-enabled-brutal-mass-detention-and-surveillance-in-china-internal-documents-show/

Kania, E. B. (2018). The dual-use dilemma in China's AI development. In *Technological entanglement: Cooperation, competition and the dual-use dilemma in artificial intelligence* (pp. 08–09). Australian Strategic Policy Institute.

Keene, J. R., Shoenberger, H., Berke, C. K., & Bolls, P. D. (2017). The biological roots of political extremism: Negativity bias, political ideology, and preferences for political news. *Politics and the Life Sciences*, *36*(2), 37–48.

Khalil, L. (2020). *Digital Authoritarianism, China and C0VID*. Lowy Institute for International Policy.

Kilgore, J. (2022). E-Carceration, settler colonialism, and the open-air prison. In *Understanding E-Carceration: Electronic Monitoring, the Surveillance State, and the Future of Mass Incarceration* (pp. 140–152). The New Press.

Kirchgaessner, S., Evans, R. and Hughes, S. (2020). UN rapporteur condemns UK hosting of Israeli spyware firm. *The Guardian*. https://www.theguardian.com/world/2020/feb/07/un-rapporteur-condemns-uk-hosting-of-israeli-spyware-firm

Kubovich, Y. (2022). Israeli Troops' New Quota: Add 50 Palestinians to Tracking Database Every Shift. *Haaretz*. https://www.haaretz.com/israel-news/2022-03-24/ty-article/.premium/soldiers-not-allowed-off-shifts-until-they-enter-50-palestinian-names-in-database/00000180-5ba7-d97e-a7fb-7bf7361c0000

Lewis, K. (2021). Social media platforms are complicit in censoring Palestinian voices. The Conversation.https://theconversation.com/social-media-platforms-are-complicit-in-censoring-palestinian-voices-161094

Lindblom, C.E. (1982). Another state of mind. *American Political Science Review*, *76*(1), pp.9-21.

Lindley, D. (2025). Exposed in Translation: Between Hebrew and English media narratives, Israel hides its war crimes confessions. *The New Arab*. https://www.newarab.com/opinion/between-hebrew-and-english-israel-hides-war-crimes-confessions

Lippmann. W. (1922). *Public Opinion*. The Macmillan Company. https://en.wikisource.org/wiki/Public_Opinion

Loewenstein, A. (2023). The *Palestine Laboratory: How Israel Exports the Technology of Occupation Around the World*. Verso.

Loewenstein, A., & Corbyn, J. (2024). The Palestine Laboratory: An Update. In R. Michie, A. Feinstein, & P. Rogers (Eds.), *Monstrous Anger of the Guns: How the Global Arms Trade is Ruining the World and What We Can Do About It* (1st ed., pp. 62–66). Pluto Press.

Lukes, S. (1974). *Power: A Radical View*, Macmillan.

Lyon, D. (2019). State and Surveillance. In *Governing Cyberspace during a Crisis in Trust: An essay series on the economic potential — and vulnerability — of transformative technologies and cyber security* (pp. 21–25). Centre for International Governance Innovation.

Margetts, H., John, P., Hale, S., & Yasseri, T. (2016). From Political Turbulence to Chaotic Pluralism. In *Political Turbulence: How Social Media Shape Collective Action* (pp. 196–228). Princeton University Press.

Markowski, R. (2020). On Complexity and Simplism. In H. K. Anheier & I. Begg (Eds.), *Ralf Dahrendorf and the European Union 2030: Looking Back, Looking Forward* (pp. 91–98). LSE Ideas.

Martinez, E.C. (2025). EU sanctions against Israel: here's what's on the table. The Conversation. https://theconversation.com/eu-sanctions-against-israel-heres-whats-on-the-table-260982

Mayfield, M., & Roaten, M. (2021). Israeli Firm Delivers Advanced Targeting System. *National Defense*, *105*(811), 13.

Mckeon, M. (2004). Parsing Habermas's "Bourgeois Public Sphere." *Criticism*, *46*(2), 273–277.

McMurray, J. (2015). The paradox of information and voter turnout. *Public Choice*, *165*(1/2), 13–23.

Missile Technology Control Regime (MTCR). (2017). Annex Handbook. https://www.mtcr.info/download/pictures/5b/4x3ixi033jhup4yyjjuotfb7074as4/mtcr-handbook-2017-indexed-final-digital.pdf

Morgus, R. (2019). The Spread of Russia's Digital Authoritarianism. In N. D. Wright (Ed.), *Artificial Intelligence, China, Russia, and the Global Order* (pp. 89–97). Air University Press.

Müller, J.-W. (2016). The EU's Democratic Deficit and the Public Sphere. *Current History*, *115*(779), 83–88.

Nanz, P. (2018). Public Sphere. In H. Brunkhorst, R. Kreide, & C. Lafont (Eds.), *The Habermas Handbook* (pp. 605–609). Columbia University Press.

Nelson, N., Speranza, L., Deni, J. R., Alden, C., Brattberg, E., Cliff, R., Duckenfield, M., & Ellis, R. E. (2022). Security Risks: Dual-Use Technology in Europe. In *China, Europe, and the Pandemic Recession: Beijing's Investments and Transatlantic Security* (pp. 151–198). Strategic Studies Institute, US Army War College.

Norwegian Refugee Council. (2018). *Gaza: The world's largest open-air prison.* https://www.nrc.no/news/2018/april/gaza-the-worlds-largest-open-air-prison

OCHA. (2025). *West Bank Movement and Access Update*. https://www.ochaopt.org/sites/default/files/Factsheet%20Booklet_Movement_and_Access.pdf

Oded, A. (2010). Africa in Israeli Foreign Policy—Expectations and Disenchantment: Historical and Diplomatic Aspects. *Israel Studies*, *15*(3), 121–142

OFTA. (2025). *Operation Find Them All*. https://ofta.cellebrite.com

OHCHR. (2025). A/HRC/59/23. Human rights situation in Palestine and other occupied Arab territories. From economy of occupation to economy of genocide Report of the Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967, Francesca Albanese.https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/sessions-regular/session59/advance-version/a-hrc-59-23-aev.pdf

OIP. (2025a). OIP selected to build spectrometer for ESA EnVision mission to Venus. https://oipspace.be/2025/05/28/venspec-h-contract-signed/

OIP. (2025b.) Company Profile. https://oipspace.be

Onuf, N. (2002). Institutions, Intentions and International Relations. *Review of International Studies*, *28*(2), 211–228.

Palan, R. (2000). A World of Their Making: An Evaluation of the Constructivist Critique in International Relations. *Review of International Studies*, *26*(4), 575–598.

Penney, J., McKune, S., Gill, L., & Deibert, R. J. (2018). Advancing Human-Rights-by-Design in the Dual-Use Technology Industry. *Journal of International Affairs*, *71*(2), 103–110.

PI. (2025). *Examples of Abuse Timeline*. https://privacyinternational.org/abusetimeline

Prime Minister's Office. (2025). *PM Netanyahu's remarks at the "Fifty States – One Israel" Event at the Ministry of Foreign Affairs, with the largest delegation of American legislators to ever visit Israel.* https://www.gov.il/en/pages/event-one-150925

Research and Markets. (2025). *Border Security System Market by Platform Type (Fixed Surveillance Systems, Portable Surveillance Systems, Unmanned Aerial Vehicles), Technology (Biometric, Iot, Rfid), Application, Deployment Mode, End User - Global Forecast 2025-2030.* https://www.researchandmarkets.com/reports/6011062/border-security-system-market-platform-type?utm_source=GNE&utm_medium=PressRelease&utm_code=kn9fvt&utm_campaign=2031314+-+Global+Border+Security+System+Market+Set+to+Surpass+%24111+Billion+by+2030+Amid+Heightened+Global+Security+Threats+and+Rapid+Developments+in+Biometric+Identification%2c+UAVs%2c+and+Cybersecurity+Solutions&utm_exec=chdomsai

Rowland, A. L. (2016). Life-Saving Weapons: The Biolegitimacy of Drone Warfare. *Rhetoric and Public Affairs*, *19*(4), 601–628.

Sample, C., Justice, C., & Darraj, E. (2019). A Model for Evaluating Fake News. *The Cyber Defense Review*, 171–192.

Senor, D. & Singer, S. (2009). *Start-Up Nation: The Story of Israel's Economic Miracle*. Twelve. https://ia600509.us.archive.org/7/items/TheLeanStartupErickRies/start-up_nation_the_stor.pdf

Shadle, M. A. (2011). Constructivism. In *The Origins of War: A Catholic Perspective* (pp. 75–94). Georgetown University Press.

Shankar, P., Dixit, P. and Siddiqui, U. (2023). Are social media giants censoring pro-Palestine voices amid Israel's war? *Al Jazeera*. https://www.aljazeera.com/features/2023/10/24/shadowbanning-are-social-media-giants-censoring-pro-palestine-voices

Shewring, E. (2025). *Israel's Spyware Law: A Step Towards Authoritarianism?* German Institute of Global and Area Studies (GIGA).

Shlaim, A. (2024). Israel's War on Gaza. In J. STERN-WEINER (Ed.), *Deluge: Gaza and Israel from Crisis to Cataclysm* (pp. 13–34). OR Books.

Silver, L., Fagan, M., Huang, C., & Clancy, L. (2024). Citizen behavior and individual rights and equality. In *What Can Improve Democracy?* (pp. 59–69). Pew Research Center.

Simon, J., & Mahoney, R. (2022). State Surveillance. In *The Infodemic: How Censorship and Lies Made the World Sicker and Less Free* (pp. 80–101). Columbia Global Reports.

Simons, M. (2025). Israeli spyware company CEO testifies in Meta damages trial. *Courthouse News Service*. https://www.courthousenews.com/israeli-spyware-company-ceo-testifies-in-meta-damages-trial/

Sivakumar, S., & Lukose, L. P. (2017). How to Read, Assess and Write A Research Article. *Journal of the Indian Law Institute*, *59*(2), 123–152.

SIPRI. (2023). *The SIPRI Top 100 arms-producing and military services companies in the world, 2023*. https://www.sipri.org/visualizations/2024/sipri-top-100-arms-producing-and-military-services-companies-world-2023

Steiner, G. (1986). Language Under Surveillance: The Writer and The State. *The New York Times*. https://www.nytimes.com/1986/01/12/books/language-under-surveillance-the-writer-and-the-state.html

The American Immigration Council. (2025). ICE to Use ImmigrationOS by Palantir, a New AI System, to Track Immigrants' Movements. https://www.americanimmigrationcouncil.org/blog/ice-immigrationos-palantir-ai-track-immigrants/

The Hague Code of Conduct against Ballistic Missile Proliferation (HCOC). (2002). Text of the HCoC. https://www.hcoc.at/what-is-hcoc/text-of-the-hcoc.html

Tkacheva, O., Schwartz, L. H., Libicki, M. C., Taylor, J. E., Martini, J., & Baxter, C. (2013). The Internet in China: Threatened Tool of Expression and Mobilization. In *Internet Freedom and Political Space* (pp. 93–118). RAND Corporation.

UK Government. (2025). Country policy and information note: social media, surveillance and sur place activities, Iran. https://www.gov.uk/government/publications/iran-country-policy-and-information-notes/country-policy-and-information-note-social-media-surveillance-and-sur-place-activities-iran-april-2025-accessible

UN. (1949). Geneva Convention Relative to the Protection of Civilian Persons in Time of War of 12 August 1949. https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.33_GC-IV-EN.pdf

UN. (1954). Convention for the Protection of Cultural Property in the Event of Armed Conflict and Protocol I. https://treaties.un.org/doc/Publication/UNTS/Volume%20249/volume-249-I-3511-English.pdf

UN. (1968). Treaty on the Non-Proliferation of Nuclear Weapons (NPT). https://treaties.unoda.org/t/npt?_gl=1*136txtx*_ga*NzMxMzE2MTc0LjE3NTQwMjg0NzA.*_ga_TK9BQL5X7Z*czE3NTQxMTQ1NzYkbzIkZzEkdDE3NTQxMTU4MzYkajYwJGwwJGgw

UN. (1972). Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction. Opened for Signature at London, Moscow and Washington. 10 April 1972. https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.37_conv%20biological%20weapons.pdf

UN. (1976). Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (ENMOD). https://treaties.un.org/doc/Treaties/1978/10/19781005%2000-39%20AM/Ch_XXVI_01p.pdf

UN. (1977a). Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), of 8 June 1977. https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.34_AP-I-EN.pdf

UN. (1977b). Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts

(Protocol II), of 8 June 1977. https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.35_AP-II-EN.pdf

UN. (1993). Convention on the prohibition of the development, production, stockpiling and use of chemical weapons and on their destruction, Paris 13 January 1993. https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.42_Conv%20Chemical%20weapons.pdf

UN. (1996). Comprehensive Nuclear-Test-Ban Treaty https://treaties.unoda.org/t/ctbt?_gl=1*1ccxsg0*_ga*NzMxMzE2MTc0LjE3NTQwMjg0NzA.*_ga_TK9BQL5X7Z*czE3NTQxNTgxMTgkbzMkZzEkdDE3NTQxNTgyNTAkajYwJGwwJGgw

UN. (1997). Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction, 18 September 1997. https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.44_convention%20antipersonnel%20mines.pdf

UN. (2000). Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict. https://childrenandarmedconflict.un.org/tools-for-action/optional-protocol/

UN. (2005). Mine Action and Effective Coordination: The United Nations Inter-Agency Policy. https://www.mineaction.org/sites/default/files/documents/maec.pdf

UN. (2008). Convention on Cluster Munitions. https://treaties.un.org/doc/Publication/CTC/26-6.pdf

UN. (2013). The Arms Trade Treaty. https://treaties.un.org/doc/Treaties/2013/04/20130410%2012-01%20PM/Ch_XXVI_08.pdf

UN. (2017). Treaty on the Prohibition of Nuclear Weapons. https://treaties.unoda.org/t/tpnw?_gl=1*6u2ubx*_ga*NzMxMzE2MTc0LjE3NTQwMjg0NzA.*_ga_TK9BQL5X7Z*czE3NTQxNTgxMTgkbzMkZzEkdDE3NTQxNTgyNTAkajYwJGwwJGgw

UN. (2025a). UN Mine Action Service (UNMAS). https://www.unmas.org/en

UN. (2025b). UN Safeguard Programme. https://unsaferguard.org

UNESCO. (1999). Second Protocol to the Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict. https://unesdoc.unesco.org/ark:/48223/pf0000130696

UNGA. (2002). Measures to Prevent Terrorists from Acquiring Weapons of Mass Destruction. A/C.1/57/L.49/Rev.1. https://digitallibrary.un.org/record/476446?v=pdf

UNGA. (2010). Women, Disarmament, Non-proliferation and Arms Control. Resolution 65/69. https://docs.un.org/en/A/RES/65/69

UNGA. (2023). Youth, Disarmament and Non-Proliferation. Resolution 78/31. https://docs.un.org/en/A/RES/78/31?_gl=1*1ikzqo7*_ga*NzMxMzE2MTc0LjE3NTQwMjg0NzA.*_ga_TK9BQL5X7Z*czE3NTQxNjM4MDEkbzQkZzAkdDE3NTQxNjM4MDEkajYwJGwwJGgw

UNODA. (1980). Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects. https://treaties.unoda.org/t/ccw

UNSC. (1988). Resolution 620. Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons (UNSGM). https://docs.un.org/en/s/res/620(1988)

UNSC. (2004). Resolution 1540. https://docs.un.org/en/S/RES/1540(2004)

VRI. (2025). OIP Space Instruments. https://vri.vlaanderen/en/members/oip-sensor-systems/

Wallerstein, M. B. (1991). Controlling Dual-Use Technologies in the New World Order. *Issues in Science and Technology*, *7*(4), 70–77.

Ward, I. (1997). How Democratic Can We Get?: The Internet, the Public Sphere, and Public Discourse. *JAC*, *17*(3), 365–379.

Wæver, O. (2011). Politics, security, theory. *Security Dialogue*, *42*(4/5), 465–480.

Wendt, A. (1992). Anarchy is what States Make of it: The Social Construction of Power Politics. *International Organization*, *46*(2), 391–425.

Who Profits. (2018). "Big Brother" in Jerusalem's Old City: Israel's Militarized Visual Surveillance System in Occupied East Jerusalem. https://www.whoprofits.org//writable/uploads/old/uploads/2018/11/surveil-final.pdf

Who Profits. (2025). *Elbit Systems*. https://www.whoprofits.org/companies/company/3794

Winston, E. A., Lee, R. G., Monikowski, C., Peterson, R., & Swabey, L. (2023). Contextualizing Assessment. In *Beyond Equivalence: Reconceptualizing Interpreting Performance Assessment* (pp. 49–58). Gallaudet University Press.

Wright, N. D. (Ed.). (2019). Artificial Intelligence and Domestic Political Regimes: Digital Authoritarian, Digital Hybrid, and Digital Democracy. In *Artificial Intelligence, China, Russia, and the Global Order* (pp. 21–34). Air University Press.

Yasur, N. and Ring E. (2024). Drowning in the Flood Social Media Platforms' Management of Harmful and Pro-Terror Content During the October 7th Attack and the Israel-Hamas War. Israel Internet Association. https://en.isoc.org.il/wp-content/uploads/2024/06/ISOC-IL-drowning-in-the-flood-2024.pdf

Zahra, R. (2023). Israel helps other countries to spy on their own citizens. *Middle East Monitor.* https://www.middleeastmonitor.com/20230904-israel-helps-other-countries-to-spy-on-their-own-citizens/

Ziółkowski, M. (2004). Commodification of Social Life. *Polish Sociological Review*, *148*, 385–402.