Wired for War: The Internet, Big Tech and the Evolution of Modern-Day Conflicts

Çiğdem Işbuğa

Introduction

A survey examining the views of American citizens during the early stages of the Iraq war revealed that 77% of Americans had used the internet in conjunction with the conflict (Raine, Fox, Fallows, 2003). These findings provided insight into the ever-evolving and increasingly pivotal role of the internet during modern-day conflicts, raising profound social, ethical, and political implications. These implications are evident through the very first instances of wars taking place during the digital age, where researchers have documented technology fundamentally reshaping public perception and communication during wartime.

This introduction contextualises the presence of the internet within conflict zones by examining early studies of the internet's dual function as an emancipatory and instrumental force in the conduct of modern warfare. In particular, this report interrogates the degree of responsibility attributable to major technology corporations (collectively referred to as 'Big Tech') for their complicity in warfare, particularly during an era when corporate social responsibility has become a central concern to both consumer and investor ethics. This argument will be developed through an analysis of the roles, actions, ethical obligations, and accountability frameworks of Big Tech companies within contemporary conflicts.

From the early use of email communications to the subsequent rise of social media platforms, the internet is utilised as a key communication tool during modern day conflicts. The Kosovo war (1998-1999) occurred at a pivotal historical juncture when web engines such as Google were beginning to emerge before becoming household names.

Keenan (2001) labels the Kosovo war as the 'first internet war', citing the use of email communications by human rights activists. This phenomenon has been described as a process regarded as the 'virtualisation of war'. Keenan suggests that while the use of email communications provided a method for frontline communication, it has also risked transforming individuals consuming the news into passive spectators, desensitising them to the violence. Similar dynamics were present during the Iraq War (2003-2011), which unfolded alongside the rapid rise of social media platforms. These platforms facilitate faster and broader dissemination of wartime information while shaping public opinions in real time.

Berenger (2003) alternatively characterises the Iraq war as the 'first war in cyberspace', due to the internet's role in disseminating news. This study defines the characteristics of so-called 'new media' in the times of war (Berenger, 2003, p.179-183):

1. The convergence of websites containing material such as audio-visual messages

2. The ubiquitous nature of the internet itself

3. Agenda-setting power of new media

4. Credibility of online sources

5. Interactivity through debate and transferability of information

These characteristics illustrate how digital technologies have reconfigured communication and ethical dimensions of warfare. The most recent phase of the Israel–Palestine conflict, i.e. the war in Gaza (2023-ongoing), further demonstrates how social media platforms operate as contested spaces of representation. The Gaza war is occurring at a time when social media has been established well over a decade, as well as at a time where generative artificial intelligence (AI) is being utilised by the wider public.

The overall social implications from the use of the internet during wartime has simultaneously imposed empowerment principles and restrictions for global spectators and civilians on war zones. Moreover, there is scope for the internet to be utilised in conflicts as a weapon not only through the spread of misinformation, but also as a direct tool for warfare.

Organisations such as Human Rights Watch report on the use of digital tools by the Israeli Defence Forces (IDF) in Gaza, while other studies note the deliberate restriction of telecommunications access in the Occupied Palestinian Territories as a form surveillance of civilians and digital subjugation (Tawil-Souri and Aouragh, 2014). Such practices underpin the ethical responsibility of technology corporations indirectly and directly enabling their infrastructures to conduct military operations and assert certain narratives.

Additionally, cyberattacks constitute a prominent element of conflicts occurring in the age of the internet. This has been documented during the Russia–Ukraine conflict (2014-ongoing), where Russian operations have targeted banking, energy supply, and telecommunication infrastructures. Willett (2022) notes that military forces acknowledge the applications of technological warfare as Russian doctrine mandates integration of cyber operations into ‘full-spectrum military operations’ and ‘strategic information campaigns’ by default (p.8).

Therefore, this report seeks to examine the transformation of the internet from a communication method into an operational weapon, while analysing institutional responsibility of technology corporations that benefit from and maintain these systems.

The report is organised as follows: the first section explores the role of social media in shaping wartime communication by questioning algorithmic influence and corporate responsibility; the second examines the operational and material interactions between Big Tech and military infrastructures by focusing on artificial intelligence deployment and dedicated cyber operations. Finally, the conclusion reflects on transparency, ethical restraint, and accountability in an era where boundaries between civilian technology and digital military systems become increasingly blurred.

The Role of Big Tech in Wartime Communication: Shaping the Narrative

Since the Kosovo War, communication during wartime has evolved considerably. Social media and digital platforms are at the forefront of transforming how information circulates by shaping public perceptions of conflict. Both traditional and digital media portray the capacity of communication infrastructures in influencing public perception, albeit through vastly different mechanisms and formats. Developing this trajectory, this section critically examines how Big Tech shapes public understanding during contemporary conflicts, emphasising the ethical, epistemological, and political implications of algorithmically mediated wartime communication.

Herman and Chomsky's (2008) political economy perspective provides an analysis of the propaganda model by identifying key mechanisms:

1. Media ownership.
2. Profit orientation.
3. Dependence on advertising as the primary revenue source.
4. Reliance on business and government actors.
5. The discipline of the media through 'flak'.
6. Deliberate construction of societal divisions by designating scapegoat groups.

These dynamics, as evident in traditional media forms such as the Nazi press, are thus reflected within online platforms. When applying these features to contemporary digital ecosystems, clear parallels are seen in agenda-setting and source credibility (Berenger, 2003). While the propaganda model explains structural influence, it does not fully capture the decentralised and data-driven nature of social media platforms.

Unlike traditional media, digital platforms algorithmically push content onto feed through automated control and commodified engagement tactics. As a result, social media functions as a product and a driver of accelerated digital communication. This places greater emphasis on ethical responsibilities allocated to platforms mediating wartime information.

Rosa (2010) describes one of the features of technological accelerations as the speeding up of intentional and goal-orientated process of communication (p. 82), mostly attributed to the globalised nature of the internet. This is exemplified by social media's rapid dissemination of information in a globalised environment, and its resulting outcomes on the formation of public conflict perceptions.

Rosa (2010) distinguishes three distinct categories of acceleration: social change, technological acceleration, and the acceleration of the pace of life. These categories are interlinked by economic, cultural and structural factors. Rospigliosi and Raza-Mejia (2021) directly frame social media use

within Rosa's acceleration paradigm, linking social change and pace of life outcomes of social media use to economic, cultural, and structural factors.

Moreover, Bridle (2018) argues that the acceleration of technology has led to a collapse of societal global consensus, resulting in social divisions, ethnic conflicts, and unprecedented threats (p. 10). The speed of information creates uncertainty; many sources want to be the first to break news to the public and drive website traffic, which can lead to the blurring of credibility. For instance, Virilio (1995) uses the concept of 'information (super) highways' to illustrate the inherent risk misinformation poses from the 'absolute velocity of electronic data' (p.3) from virtualised societies. Both perspectives provide foundational insight into how the rapid circulation of information fosters uncertainty, with platforms competing for immediacy often at the expense of precision of information.

The vast volume of information generated online has led to the facilitation of contemporary conflicts. Pentina and Tarafdar (2014) stipulate social media's role in news consumption has ultimately fuelled 'information overload' by exposing individuals to 'ever-increasing barrage of news content' (p. 212). Baudrillard's (1981) perspective on hyperreality cements this notion by recognising that the representation of reality and reality itself have collapsed. Individuals struggle to distinguish reality from media representations, as media outlets no longer merely reflect, but instead actively construct the hyperreal.

In the context of wartime communication, this form of collapse is present in the form of algorithmic 'hyperreality'. Big Tech has the authority to govern what content is perceived as real and cultivate exposure. However, it can be argued that not all individuals experience this equally, as digital platform usage, cultural context and media literacy shape varying perceptions of reality. Hence, the intersection of technological acceleration and hyperreality ultimately transforms perceptions into a contested terrain and positions Big Tech as an infrastructural foundation of modern conflict.

The rise of social media platforms being used as primary forms of information and news sources is apparent in modern society. The Reuters Institute and University of Oxford (Newman et al, 2025) Digital News Report indicates that social media companies dominate as a primary source for news content compared to traditional media. The report highlights, in particular, that six online networks now provide over 10% of weekly news content compared with two decades ago.

Platforms operated by technology companies such as Alphabet, ByteDance, Meta, and X (formerly Twitter) have considerable authority within global news output spaces. This quantitative shift conveys transformation in communication power and demonstrates the pivot from prominence of authority from journalistic to algorithmic models. This evolution fundamentally forms how individuals consume news modern conflicts, reflecting the patterns initially observed during the Iraq War (Fox, Raine, and Fallows, 2023).

Algorithms operate as curational mechanisms by organising content for users based on personalisation and prioritisation (Mazúr and Patakyová, 2019). Napoli (2019) notes that Facebook began prioritising posts by engagement rather than chronology from 2009 onwards. This reflects the broader shift from passive content consumption to engagement-driven distributions, resulting

in altered information ecosystems. Conversely, algorithmics are not only influenced by user activity, but it is also altered by decisions made by actors within technology companies themselves.

Gram and Andrejevic's (2024) computational analysis conducted on the algorithmic bias on Platform X during the 2024 US election found system-wide modifications coinciding with executive chairman Elon Musk's endorsement of Donald Trump, indicating increased visibility and influence of Republican-affiliated accounts. Conclusions of the study suggest that the presence of algorithm bias favouring pro-Republican accounts were prevalent (p.19-20). These findings demonstrate the nexus between corporate governance, algorithmic engineering, and political influence, thus reinforcing the need for ethical accountability in algorithm design.

Early Internet use has enabled public engagement with live updates from warzones. This is demonstrated through email exchanges during the Kosovo War (Keenan, 2001) and war blogs authored by Iraqi citizens (Matheson and Allan, 2009). Eventually, Web 2.0 emerged as a central infrastructure for communication and mobilisation (Frangonikolopoulos and Chapsos, 2012). Conversely, immediacy is not synonymous with transparency. This is due to algorithmic curation exhibiting hierarchies of visibility, where factual reliability is often neglected.

For instance, Maharani's (2024) qualitative social media analysis of perceptions of the Israeli-Palestinian conflict illustrates the nuanced ways social media networks operate in exerting influence and reach within the context of the conflict. The platform X, for example, is used to facilitate immediate mobilisation among users through debates and updates. In contrast, Facebook and Instagram encourage longer-form discussions and community building, and provide a personal element through storytelling. Such distinctions highlight how engagement mechanisms differ in mediating conflict narratives, expanding the sociotechnical nature of wartime communication.

Despite these contrasts, algorithmic systems increasingly amplify content visibility according to engagement metrics, resulting in the creation of echo chambers and reinforcement of social divisions (Maharani, 2024) The accelerated circulation of information exacerbates the risk of misinformation and censorship. Such findings demonstrate that algorithmic design is inherently non-neutral, raising pressing ethical concerns surrounding accountability for the operation of platforms during wartime.

The presence of algorithmic influence further applies to the exhibition of modern-day conflicts online. It can be argued that algorithms have a tendency to prioritise emotionally or sensational content. For example, Meta issued an apology after users reported increased violent content on the Instagram Reels Feature (The Guardian, 2025); the increase was attributed to the algorithm promoting the content onto user pages.

Similarly, Ertuna (2023) examines the 'TikTokisation' of the war in Ukraine, observing the platform's 'For You' algorithm procuring thousands of associated posts, and generating billions of views. Heřmanová et al (2025) attributes the increase in algorithmic prioritisation due to their tragic subject matter. By prioritising emotionally charged or sensational content, these algorithms enable further amplification, incentivising the system to reward content aligned with preferences.

An alternative argument emphasises how citizens in warzones can strategically leverage algorithms to expand outreach, creating a contrast with limited email outreach in Web 1.0. For instance, Kahmis and Dogbatse (2024) identify the instrumental role of social media in amplifying counter-narratives during the Gaza war. This reflects the participatory and decentralised nature of digital activism, as citizens are able to provide live updates while simultaneously gaining substantial global visibility through algorithmically boosted hashtags. Moreover, Kahmis and Dogbatse note further benefits stemming from online communities organising crowdfunding initiatives, such as 'eSims for Gaza'.

These examples, alongside the growing prominence of content from Ukrainian citizens on TikTok, demonstrate the use of civilian communication during wartime, increasing interactivity and transnational solidarity. Nonetheless, concerns encompassing algorithm biases and political influence encapsulate the responsibility of technology companies managing algorithmic output.

Moreover, scholars point out that algorithmic bias within tech companies continues to oppress activism despite the use of the platforms to spread awareness of contemporary conflicts. Abushbak, Majeed, and Sinha's (2023) examination of digital spaces shaped by civilian activism on Instagram reveals that, although the platform empowers the private citizen to be an actor in the war, it simultaneously imposes barriers to visibility at the same time. The study identifies Palestinian activists reporting suppressed hashtags, restricted visibility, and (in some instances) account removals altogether.

Such censorship of civilian content is regarded as a form of 'algorithmic gatekeeping' (p. 165). In response to reports on the matter by the Business and Human Rights Resource Centre (2025), Meta claimed it 'strongly disagrees' with allegations that the company facilitated an Israeli-led censorship campaign on its platforms. Nevertheless, Ekō (2024) published a report revealing that Meta profited from advertisements promoting the IDF by permitting fundraising campaigns for military equipment despite it going against the company's rules.

The report identified 98 advertisements targeting audiences in the US and Europe to raise funds for assault rifles and drone technologies. Further instances of censorship are seen at the height of Israeli aggression on the Gaza Strip on Alphabet's YouTube platform. YouTube had reportedly restricted access to the live broadcast on the Al Jazeera YouTube channel, while simultaneously deleting media clips published on Palestinian channels (Miladi and Miladi, 2023). In addition, the word 'Palestinians' in auto-translated subtitles for Turkish and Arabic was translated to 'Terrorists' instead. With civilian restriction and narrative dissemination occurring across different social media platforms, these documented cases present a striking contrast to the censorship experienced by Palestinian civilians and activists against platforms being slow to remove fundraising advertisements directly on the same social media platforms, instead highlighting Big Tech's selective moderation practices and exercise of digital visibility power.

To develop a comprehensive understanding of corporate accountability in shaping modern conflict narratives, it is essential to further explore legal arguments and ethical approaches to algorithmic bias. Sun (2023) argues that the responsibility of social media companies needs to be ultimately redefined through the recognition of 'right to know' algorithms (p. 38). This change

would promote transparency and accountability, benefiting both society and platform users by establishing the public sector role that major social media companies perform in their functions (p. 39).

In contrast, Balkin (2020) rejects the notion that social media services should be treated as public utilities as algorithmic bias. Instead, he advocates for incentive-based models for regulation for the privately owned companies, noting that the platforms already apply independent rules for civility, safety, and behavioural norms (p. 78). However, despite internal standards being established, platforms continue to prioritise engagement and profitability, especially when mediating content relating to contemporary conflicts.

This is further stipulated by the Oversight Board's (2025) findings on Meta's content removal procedures being inconsistent with its human rights responsibilities. The findings emphasise lack of due diligence during instances when critical content intended to protect civilians during conflict situations was removed by the company. Therefore, the very rules designed to promote online safety may have inadvertently perpetuated harm by enforcing barriers for civilians who depend on platform communication during wartime.

Alternatively, Buzzi argues for a Responsibility to Protect (R2P) approach for social media companies, highlighting the example of the liberalisation of the telecommunications sector being a key factor of political changes that took place in Myanmar in 2011, enabling the widespread availability of internet access. The emergence of social media platforms in particular demonstrated that platforms had transformed into spaces for both human rights activism and human rights abuses against minority groups to take place. The lack of social media platform governance is highlighted in the study as a key component in inciting violence against vulnerable individuals, as the study provides the example of Facebook in particular as being slow in developing an effective response to inflammatory posts. These dynamics raise profound ethical and legal questions regarding the advocacy of corporate self-regulation to safeguard vulnerable populations in conflict zones.

This section has examined the role of big tech companies as simultaneous enablers and gatekeepers of wartime communication. In particular, this section zones in on algorithmic power which determines narratives on credibility and visibility. It has explored the ways in which algorithm bias can undermine the advantages of increased exposure restricting civilian journalism and transforming information into a weaponised commodity.

In this context, social media companies assume the role of arbiters of information, determining which voices are amplified or suppressed. Herman and Chomsky's propaganda model can be applied to the structural forces underlying algorithmic hierarches. Studies on the Gaza War exemplify such processes and reveal how digital barriers enforced on activists and civilians constitute a form of informational soft power.

Applying Rosa's (2010) theory of acceleration directly corresponds towards how the shift of information has transformed conflict engagement. Ultimately, the ethical responsibility for mitigating harm, ensuring accurate representation and safeguarding civilians lies notably with Big

Tech companies due to their control over information and algorithmic flow of content. The following section shall describe instances of the internet being used as a tool during wartime.

The Role of Big Tech in Wartime: Live Deployment

While the role of Big Tech companies has become increasingly politicised through global outreach, these firms have also assumed a direct and operational function within the defence industry. The term 'virtual warfare' is widely used to describe the use of high-technology psychological operations (psyops), autonomous weapon systems and cyber-attacks on critical digital infrastructure (González, 2023). Moreover, the origins of the internet itself are closely linked to military innovation, most notably through the development of the Advanced Research projects Agency Network or ARPANET by the United States Department of Defense (Maaser and Verlaan, 2022). This historical link suggests that the internet's early conception was inherently intended for military objectives.

The outreach of social media networks has enabled big tech companies to consolidate control over infrastructure and knowledge production, while dual-use technologies have transformed such firms into key components in the digital-military-industrial complex (Coveri, Cozza, and Guarasico, 2025). Several scholars argue that the growth in prominence places increased scrutiny of Big Tech's responsibility for direct weaponisation of its technologies and services.

As discussed in the previous section, platforms already bear responsibility over how they facilitate wartime communication and shape conflict narratives through algorithmic power. At the same time, military operations worldwide increasingly recognise the strategic advantages of algorithmic systems. For instance, Russia has integrated cyberwar tactics into its strategic information campaigns and broader military operations (Willet, 2022). Such developments raise serious ethical concerns regarding Big Tech's provision of technological infrastructure that enables or facilitates military operations, rendering these companies as complicit in human rights violations.

This section examines the weaponisation of the internet during wartime and the ethical implications for Big Tech companies involved in or facilitating acts of digital violence. The first part explores the use of the internet itself as a tool for virtual warfare through focusing on misinformation and propaganda campaigns conducted by state and non-state actors to foster social division. The second part takes a descriptive approach in analysing the use of online tools in cyberattacks, artificial intelligence (AI), and surveillance systems targeting civilian and military infrastructure. The section then concludes by assessing corporate complicity and accountability in facilitating contemporary conflicts.

As established in the section above, social media functions as a central arbiter in dissemination and mediation of wartime information. This has resulted in entire military operations revolving around the weaponisation of social media through facilitation of strategic misinformation. A report by the Oxford Internet Institute (Bradford, Bailey, and Howard, 2020) investigated the global organisation of social media manipulation by political parties and government actors. The report's

findings revealed that 81 countries had used social media networks to spread computational disinformation and propaganda.

In particular, a key feature to computational propaganda is cyber-troop campaigns orchestrated by political or government entities having contractual partnerships with private strategic communication firms (p. 2). Computational propaganda is defined as the use of algorithms, human curation, and automation to intentionally distribute misinformation over social media platforms (Woolley and Howard, 2017). Such interference in algorithmic output shifts the attention to the measures implemented by Big Tech companies to preventing influence.

These operations frequently employed 'sock puppet' accounts designed to manipulate audiences and further certain political narratives. To identify such campaigns and patterns of automated activity, McBride, Gold, and Stricklin (2020) recognise an overlap between bots, social media bots, and internet trolls, defining social media bots as automated accounts that post repeatedly to intentionally spread disinformation (p. 9).

The interference of bots on platforms blurs the boundaries between military strategies and digital propaganda, corresponding with Baudrillard's (1981) notion of hyperreality (Morris, 2020), and presenting further implications of covert cyber warfare. Moreover, the propagandistic feature of new media is replicated in communicational methods (Berenger, 2003). This new form of propaganda has the ultimate objective to employ social media platforms as an active instrument for manipulating public perceptions (Woolley and Howard, 2017). Bots exemplify this objective by having the capacity to post content at high rates and regular intervals compared to human users, exploiting engagement-based algorithms to amplify information campaign narratives.

A widely cited example of such activity is the deployment of Russian botnets to propagate misinformation campaigns. Beskow and Carley (2020) document the interference of Russian bots in the United States by noting the significant role of the Russian Internet Research Agency (IRA) in St. Petersburg in conducting the campaigns. The IRA participates in information operations on social media on the behalf of Russian businesses and the government. In 2019, the Special Counsel Investigation 'Mueller' report named the IRA as a key facilitator in the propagation of misinformation surrounding the 2016 presidential election (Beskow and Carley, 2020, p.4). The IRA-operated accounts maintained an active presence within anti-immigration groups, religious spaces, and political activist networks across multiple social media platforms, ranging from Twitter to YouTube.

Combined with the interference of political views from actors within technology companies, the existence of Russia's IRA indicates increased political influence and a recognition of methods to exploit algorithmic systems. The continued use of bot networks persists during the ongoing Russia-Ukraine war, further demonstrating the intensification of the weaponisation of the internet and emergence of digital information warfare. Marigliano, Xian Ng, and Carley (2024) analyse Russia's bot-driven campaigns, revealing how automated strategies exert influence on social media narratives surrounding the conflict. The narratives were aimed to manipulate moral values to increase polarisation and ethical ambiguity in modern information warfare.

Abbas and Ibrahim's (2025) qualitative mixed-methods research into social media use in the Sudan War provides further insight into the role of social media as an essential tool for military and political mobilisation. The study highlights in particular that the Sudanese Armed Forces (SAF) and the Rapid Support Forces (RSF) utilise social media platforms as an active digital warfare strategy component. Targeted messaging campaigns are deployed to gain public sympathy and justify wartime actions. In addition, Abbas and Ibrahim note that the presence of the accounts of the factions enable them to counter opposing narratives and spread misinformation. Policy recommendations from the study pertain to the increase of digital governance and the enhancement of social media platform accountability.

The militarisation of social media ecosystems raises pressing question about the responsibility of social media companies whose platforms are used to facilitate cyber-troop activity and computational propaganda. As discussed regarding algorithmic responsibility, it can be similarly argued that robust regulation and moderation could mitigate bot activity on social media networks.

Santos-Okholm, Fard, and ten Thij (2024) analysed posting patterns of Russian propaganda media following the European Union's decision to implement a geo-block on Russian media outlets. The study proposes that targeted censorship holds potential in limiting misinformation campaigns on major platforms. Nonetheless, a tension exists between defence and freedom of expression.

A degree of responsibility remains allocated to Big Tech companies whose infrastructures enable government and private actors to manipulate public opinion and effectively transform digital platforms into active instruments of warfare through bot activity. Other scholars, however, extend this critique beyond disinformation, instead focusing on Big Tech's prominent role in enabling direct forms of digital weaponisation through surveillance and the use of artificial intelligence.

The use of the internet to conduct cyberattacks during modern day conflicts poses grave threats to national security and the stability of critical infrastructure. Hodges and Creese (2015) define cyberattacks as electronic assaults targeting enterprises, individuals or systems with the intention to disrupt, corrupt or steal assets. Cyberattacks are often differentiated according to types, objectives, and stage (Biju, Gopal, and Prakash, 2019). Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, for example, overrun system resources to prevent the server from responding to legitimate requests, resulting in essential network resources being rendered unavailable (p. 4,849). Other common forms include the deployment of malware or malicious software installed without user consent. Malicious code such as viruses and worms compromises sensitive data, aiming to disrupt critical operations (p. 4,851).

Zeadally and Flowers (2014) indicate that DDoS attacks are frequently used by small nations or non-state actors because they are relatively inexpensive to launch compared to traditional military operations. Although, more advanced cyberattacks require specialised training (p. 18). As indicated above, many states now integrate cyber dimensions directly into their military strategies (Willett, 2022), recognising that cyberwarfare provides a cost-effective, disproportionate means of power projection. This evolution allows nations to launch large-scale operations targeting critical

infrastructure, such as power grids, financial systems, and communication networks without the need to deploy physical weaponry.

Lu (2015) warns that the cyberattacks on critical infrastructure have the ability to exceed those of conventional warfare, potentially replicating damage 'worse than a weapon of mass destruction'. For instance, a successful cyberattack on a nuclear reactor has the potential to cause radiological dispersal, mass casualties, psychological trauma, and long-term contamination (p. 52). The trend of such cyberattacks not only blurs the boundary between civilian and military digital spaces, but also raises urgent ethical question regarding the complicity of technology companies whose infrastructure and services may be co-opted for cyberwarfare.

While the extent of cyberattacks may appear abstract, the expansion of military cyber capabilities demonstrates an increasing willingness among states to weaponise the internet itself. In June 2010, the Stuxnet malicious worm software was discovered after being suspected of targeting Iran's uranium enrichment and nuclear programme (Mueller and Yadegari, 2012). Stuxnet proved highly effective, reportedly destroying around 1,000 centrifuges, or approximately 11% of Iran's installed total, and disrupting the uranium enrichment processes (p. 1). Israel and the United States are widely speculated to be the responsible for the operation, though neither government has officially claimed any responsibility (p.3).

Bridle (2018) attributes the profound impact of cyberattacks on infrastructure to society's dependence on computational systems, therefore exposing engineered weaknesses and systemic blind spots (p. 37-38). The automation of critical societal functions has, in turn, created new opportunities for the development of digitally mediated military tactics. Although, the Stuxnet attack primarily targeted Iran's nuclear infrastructure rather than civilian systems, it still illustrates a decisive shift in warfare.

Since the growth of the digital-military industrial complex, the frequency and severity of cyberattacks on national infrastructure have notably increased. Eichensehr (2022) illustrates the evolution of Russian cyber operations against Ukraine, beginning with attacks between 2015 and 2016, which had caused nationwide blackouts across Ukrainian energy grids (p. 145). In the following year, it was revealed that the Russian military had used Ukrainian account software to launch a destructive malware referred to as 'NotPetya'. Rather than enabling ransom recovering, NotPetya irreversibly encrypted victims' data and caused ransom payments to be futile, resulting in a widespread global contagion that procured an estimated USD 10 billion in damages.

The sheer scale and economic devastation of NotPetya emphasises cyberwarfare's increasing appeal for defence forces. Moreover, Schulzke (2018) stipulates that responsibility is a central challenge for cyber conflict, since tracing attacks to their true origin remains politically and technically complex. This ambiguity affords military actors plausible deniability, while Big Tech infrastructures such as cloud services, software platforms, and operations systems remain integral to the smooth running of the operations.

The integration of AI into military systems further deepens Big Tech's direct role in the weaponisation of the Internet. Developments of AI over the past two decades have created new opportunities for both Big Tech companies and defence forces. AI refers to the subpart of

computer science concerned with enabling machines with the sophistication to act intelligently within increasingly wider realms (Nilsson, 1980). Applications of AI range from the use of speech recognition, computer vision, expert systems, and decision making (McCarthy, 2004). In more recent years, however, generative AI has become the most widely form, capable of production imagery, text, and other media outputs from prompts from human users.

The development of AI research emerged post-WWII, when scholars began developing theoretical frameworks for intelligence machines following Alan Turning's lecture on machine reasoning (McCarthy, 2004). Contemporary advances in generative AI have brought these technologies in the public sphere as companies such as OpenAI and Alphabet have commercialised AI systems, finding an aspect to profit from and commercialise the technology.

AI development offers benefits through healthcare decision making and diagnostic systems (Hamet and Tremblay, 2017, it simultaneously poses complex ethical and political considerations in relation to contemporary conflicts. Arogyaswamy (2020) identifies key risks related to AI integration to military operations, highlighting concerns surrounding human oversight, accountability, and cyber vulnerabilities. The Center for Security and Emerging Technology (Foster and Arnold, 2020) exemplifies the increase for ethical considerations, noting that the U.S. Department of Defense had explicitly designated AI as a critical component of national security strategy, further blurring the lines between civilian and military application.

The position of Big Tech companies has become instrumental in supplying the technological infrastructure which enable the development and deployment of AI within U.S. defence operations. Notably, Project Maven and the Joint Enterprise Defense Infrastructure (JEDI) are key AI-driven projects within the U.S. military (Maaser and Verlaan, 2022). Project Maven launched in 2017 as an initiative to integrate AI into military conflict scenarios, with Alphabet as a key facilitator of the project and having a reported valued of USD 250 million dollars annually (Bloomberg, 2024).

Such contracts demonstrate the persistence of defence institutions in embedding AI technologies into cyberwarfare and their reliance on private technology companies. However, this link raises pressing questions regarding the ethical application of AI in active conflict zones. Husain (2021) distinguishes AI's presence in warzones, contrasting to that of nuclear weapons due to its scientific nature. Nuclear operations unlike AI, have the ability to be monitored, detected or banned. Instead, Husain (2021) theorises that 'hyperwar' AI offer strategic advantages through the deployment of small, mobile, and autonomous forces such as drones.

Recent emerging examples further illustrate the extent of Big Tech's involvement in military AI operations. Reports indicate that Amazon and Alphabet have provided AI services to the IDF under a contract valued at USD 1.2 billion, dedicated to the Nimbus project. This project supported the Israeli government's use of AI-powered tracking and facial recognition software (Coveri, Cozza, and Guarascio, 2025). Moreover, the contract allegedly included clauses preventing the companies from exercising oversight on how the technology was applied or suspended services in case of human rights violations (Abdelnour, 2023). The absence of key accountability systems highlights the degree to which Big Tech companies facilitate digital infrastructures, thereby contributing to potential human rights abuses.

Reichert (2025) further examines the integration of AI-based logistics and surveillance into the IDF's operations. Drawing on reporting by Yuval Abraham (2024), the study documents how AI systems are incorporated into the 'kill chain'. The 'kill chain' automates processes of mediated targeting, geolocation, and data surveillance (p.2-3). Approximately 2.3 million residents of Gaza were reportedly profiled within this AI programme's database which contained personal data such as age, appearance, gender, social media activity, and movement patterns (Abraham, 2024).

These findings amplify existing concerns surrounding civilian surveillance and data exploitation. Such cases highlight how Big Tech companies have become primary enablers of AI militarisation, increasing their control over massive user data ecosystems and having the financial capacity to sustain advanced research (Khanal, Zhang, and Taeihagh, 2024). Ultimately, Big Tech's direct role in military operations extends beyond complicity; it constitutes direct participation in developing technologies that perpetuate civilian oppression.

Human rights organisations, such as Amnesty International, Human Rights Watch, and the Electronic Frontier Foundation have published evidence implicating companies including Palantir Technologies in enabling violations of international law. Palantir's entire purpose was centred around providing direct support to the US Department of Defense (King, 2024). Contracts between Palantir and the Department of Defense spanning over 2024-2026 amounted to USD 1.277 billion (USASpending, 2026). This reinforces calls for preventive measures to limit AI militarisation. Sætra, Coeckelbergh, and Danaher's (2021) propose the 'AI ethicist's dilemma', presenting two potential ethical strategies for addressing Big Tech's complicity.

The first strategy focuses on internal advocacy demonstrated by employees and consumers; the second strategy takes the form of external activism through boycott driven campaigns (p. 17). An example of the first strategy can be observed in 2018, when over 3,000 Google employees signed a petition to withdraw from Project Maven resulting in the company's eventual exit (Coveri, Cozza, and Guarascio, 2025). Similarly, activist motivated boycotts, such as referring to BDS lists, and social media campaigns align with the second strategy's external focus.

Despite such efforts, the ultimate ethical responsibility remains with Big Tech itself, given its central role in securing defence contracts and developing technologies that enable the surveillance of civilians and warzone communication. A potential third strategy is situated in transparency and independent oversight, as evidenced by Microsoft's recent decision to block Israel's Unit 8200 from accessing Azure Cloud and AI services. This action followed investigative reporting from 972+, Local Call, and The Guardian, supported by Amnesty International (2024). Journalistic and academic interventions demonstrate that accountability can also be driven through research, offering alternative mechanisms to challenge Big Tech's participation in digital warfare.

The role of Big Tech in contemporary cyberwarfare and its complicity in enabling military operations is thus evident through the deep integration of technology into modern conflict infrastructures. This relationship is most prominent through defence forces adopting information warfare strategies which rely on bot activity, cyberattacks, and AI-driven surveillance systems, while simultaneously awarding lucrative defence contracts to major technology corporations.

Hunter et al (2024) further substantiate this concept by identifying the integration of AI into information warfare and influence operations across China, the United States, and Russia.

The first part of this section illustrated how social media platforms became instruments of psychological warfare. While algorithmic bias and corporate censorship exacerbate ethical concerns around representation and access to credible information, it also reinforces concerns surrounding military operations utilising social media platforms in online divisive tactics. The second part has demonstrated the direct participation of Big Tech companies in military operations through defence contracts and AI research, indicating a more involved role. The applications of AI in warfare range from automated weapons systems to extensive surveillance technologies designed to monitor populations.

Masser and Verlaan's (2022) analysis of U.S. and European technology firms within the military-industrial complex exhibits the depth of collaboration between private corporations, defence agencies, and state actors. In 2025, the Independent had reported that OpenAI, Google, and platform X's xAI were collectively awarded pentagon contracts worth around USD 200 million dollars to advance AI development, further reinforcing the entanglement.

Some scholars advocate for resolving such ethical dilemmas through internet and external reform, and by mobilising consumers, employees, and activists to challenge corporate behaviour. Conversely, other scholars contend that accountability must be enforced through independent research, wider public scrutiny, and demands for transparency. This allocates the focus on ethical responsibility back to Big Tech companies. Ultimately, Big Tech's participation in cyberwarfare reinforces structural power disproportionalities and deepens the ethical mounting concerns surrounding digital militarisation. The role of these companies extends beyond technological facilitation, as the active systems have started to blur the boundaries between civilian life, surveillance, and warfare.

Conclusion

To conclude, this report has examined the multifaceted role of Big Tech corporations in contemporary conflicts, situating activities within debates on technological sovereignty, digital barriers, and ethical accountability. This critical analysis has demonstrated that the internet has become deeply intertwined with mechanisms of warfare, surveillance, and geopolitical influence.

The first section has addressed the ethical and operational responsibilities of Big Tech firms facilitating wartime communication by emphasising how algorithmic curation, data-driven visibility, and content moderation on social media platforms shape wartime communication. While some scholars advocate for greater transparency by reconceptualising these platforms as private entities rather than public utilities (Sun, 2023), others maintain that existing moderation frameworks already perform a limited regulatory function (Balkin, 2020). Nonetheless, social media ecosystems continue to serve as both civic arenas for mobilisation and instruments of state or military information control, as exemplified in the section above. This dual application has been

particularly evident in the ongoing Israel-Palestine and Russia-Ukraine conflicts, where increased botnets and propaganda campaigns indicate the militarisation of digital information flows.

In contrast, research on internet use in contemporary conflicts occurring in territories such as Myanmar and Sudan have demonstrated a scarce amount of coverage and analysis. This is attributable to selective media coverage of conflicts and algorithm preference. Future research should aim to expand reporting to cover the role of technology companies within Myanmar and Sudan.

Further analysis extended to the complicity of Big Tech in enabling military operations highlights the development, contracting, and deployment of artificial intelligence systems. Research conducted into the use of AI in warzones realises ethical concerns regarding civilian surveillance, data extraction and automated decision-making systems deployed in conflict contexts. In the case of the Gaza War, the historical dependence on U.S.-backed ICT infrastructure illustrates what Tawil-Souri and Aouragh (2014) conceptualise as cyber colonialism; a configuration of foreign technical control that facilitates surveillance, blackmail, and disproportionate power relations.

The final discussion has engaged with potential mechanisms of resistance and accountability. Scholars recognise that methods including employee activism, consumer mobilisation, and independent cyber-policy frameworks have the ability to increase corporate accountability (Sætra, Coeckelbergh, and Danaher, 2021; Lin, Allhoff, and Abney, 2014). Yet, despite such efforts, the weaponisation and normalisation of the internet as an instrument remain entrenched. Contemporary conflicts reveal how digital infrastructures operate as both settings and instruments of war while blurring distinctions between civilian and military domains.

Ultimately, this report argues that Big Tech corporations function as key components within the digital-military-industrial complex, mediating not only the circulation of information, but also the logistics and execution of warfare itself. The technological capacities of Big Tech companies provide further instance of the amplification of state power influences, while obscuring lines of accountability.

This report demands focus on questions surrounding transparency, ethics, and corporate responsibility. Future research should aim to engage with the perspectives of diverse stakeholders, including employees, affected civilians, investors, and policymakers to assess how meaningful oversight has the potential to be achieved in an era where technological innovation and militarisation are increasingly rampant.

Bibliography

Abdelnour, S. (2023), 'Making a killing: Israel's military-innovation ecosystem and the globalization of violence', *Organization Studies*, 44(2), pp.333-337. doi: https://doi.org/10.1177/01708406221131938

Abraham, Y. (2024), '" Lavender": The AI machine directing Israel's bombing spree in Gaza'. Available at: https://www.972mag.com/lavender-ai-israeli-army-gaza/ , [Accessed: 10 October 2025].

Abushbak, A.M., Majeed, T. and Sinha, A. (2023) 'Instagram, censorship and civilian activism: The digital presence of the Israel–Palestine conflict narratives', *NIU International Journal of Human Rights*, 10(1), pp.162-171. Available at: https://www.researchgate.net/publication/368476482_Instagram_Censorship_and_Civilian_Activism_The_Digital_Presence_of_The_Israel-Palestine_Conflict_Narratives

Amnesty International. (2025) 'Israel/IOPT: Microsoft's move to block Israeli military unit's access to its mass surveillance technology is a moment for corporate reckoning'/ Available at: https://www.amnesty.org/en/latest/news/2025/09/microsoft-block-israel-military-unit-from-using-its-technology/ , [Accessed: 17 October 2025]

Arogyaswamy, B. (2020), 'Big tech and societal sustainability: an ethical framework', *AI & society*, 35(4), pp.829-840. doi: https://doi.org/10.1007/s00146-020-00956-6

Balkin, J.M. (2021), 'How to regulate (and not regulate) social media', *Journal of Free Speech Law*, 1, p.71-90. Available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/jfspl1&div=6&id=&page=

Baudrillard, J. (1981), *Simulacra and simulation*. University of Michigan press. Available at: https://0ducks.wordpress.com/wp-content/uploads/2014/12/simulacra-and-simulation-by-jean-baudrillard.pdf

Berenger, R.D. (2006). 'Introduction: War in cyberspace', *Journal of Computer-Mediated Communication*, 12(1), pp.176-188. doi: https://doi.org/10.1111/j.1083-6101.2006.00320.x

Beskow, D.M. Carley, K.M. (2020), 'Characterization and Comparison of Russian and Chinese Disinformation Campaigns', in Shu, K., Wang, S., Lee, D. Liu, H. (eds) *Disinformation, Misinformation, and Fake News in Social Media,* Lecture Notes in Social Networks. Springer. doi: https://doi.org/10.1007/978-3-030-42699-6_4

Biju, J.M., Gopal, N. and Prakash, A.J. (2019), 'Cyber attacks and their different types', *International Research Journal of Engineering and Technology*, 6(3), pp.4849-4852. Available at: https://www.researchgate.net/publication/366090166_CYBER_ATTACKS_AND_ITS_DIFFERENT_TYPES

Bloomberg. (2024), 'Inside Project Maven, the US Military's AI Project'. Available at: https://www.bloomberg.com/news/newsletters/2024-02-29/inside-project-maven-the-us-military-s-ai-project , [Accessed: 3 October 2025]

Bradshaw, S., Bailey, H. and Howard, P.N. (2020), '*Industrialized Disinformation*

2020 Global Inventory of Organized Social Media Manipulation', Oxford: Oxford Internet Institute. Available at: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/01/CyberTroop-Report-2020-v.2.pdf

Bridle, J. (2018), *New dark age: Technology and the end of the future*, London: Verso Books.

Business and Human Rights Resource Centre. (2025), 'Meta responds to allegations of facilitating Israeli-led censorship campaign', Available at: https://www.business-humanrights.org/en/latest-news/meta-responds-to-allegations-of-facilitating-israeli-led-censorship-campaign/ [Accessed: 3 October 2025]

Buzzi, C., (2021), 'Mass Atrocities in Myanmar and the Responsibility to Protect in a Digital Age', *Global Responsibility to Protect*, *13*(2-3), pp.272-296, Available at: https://brill.com/view/journals/gr2p/13/2-3/article-p272_272.xml

Coveri, A., Cozza, C. and Guarascio, D. (2025), 'Big Tech and the US Digital-Military-Industrial Complex', *Intereconomics*, 60(2), pp.81-87. Available at: https://www.intereconomics.eu/contents/year/2025/number/2/article/big-tech-and-the-us-digital-military-industrial-complex.html

Eichensehr, K.E. (2022), 'Ukraine, cyberattacks, and the lessons for international law', *American Journal of International Law*. Available at: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/ukraine-cyberattacks-and-the-lessons-for-international-law/69B36016B06998BCE1EC67C757CDF34D

Ekō. (2024), *Meta Profiting from Far-Right Genocidal Narratives and Fundraising for Israeli Military Equipment: How Meta ads support hate speech and supply military equipment to Israel*. Available at: https://aks3.eko.org/pdf/Israel_Meta_Ads_Brief.pdf

Ertuna, C. (2023), '"TikTokisation" of the War: How the War in Ukraine Was Covered on the Social Media Entertainment Platform', In *Mapping Lies in the Global Media Sphere* (pp. 75-92). London: Routledge.

Frangonikolopoulos, C.A. and Chapsos, I. (2012), 'Explaining the role and the impact of the social media in the Arab Spring', *Global Media Journal: Mediterranean Edition*, 7(2). Available at: https://www.academia.edu/2370755/Explaining_the_role_and_impact_of_social_media_in_the_Arab_Spring_

Foster, D. and Arnold, Z. (2020), 'Antitrust and Artificial Intelligence: How Breaking Up Big Tech Could Affect the Pentagon's Access to AI', *Center for Security and Emerging Technology (CSET) Issue*

Briefing. Available at: https://pdfs.semanticscholar.org/be94/6a8b502115535a406a3455e763e7a6810280.pdf

Graham, T. and Andrejevic, M. (2024), 'A computational analysis of potential algorithmic bias on platform X during the 2024 US election', *Unpublished working paper*. Available at: https://eprints.qut.edu.au/253211/ , [Accessed 17 October 2025]

Hamet, P. and Tremblay, J. (2017), 'Artificial intelligence in medicine', *metabolism*, 69, pp.S36-S40. doi: https://doi.org/10.1016/j.metabol.2017.01.011

Herman, E.S. and Chomsky, N. (2008), *Manufacturing consent*: *The political economy of the mass media*, London: The Bodley Head.

Heřmanová, M., Eriksson Krutrök, M. and Divon, T. (2025) '"The algorithm loves the war": ambivalent visibility in content creator practices during war', *Continuum*, pp. 1–17. doi: 10.1080/10304312.2025.2507777

Hodges, D. and Creese, S. (2015), 'Understanding cyber-attacks', In *Cyber Warfare*, pp. 33-60, London: Routledge. Available at: https://www.taylorfrancis.com/chapters/edit/10.4324/9781315761565-3/understanding-cyber-attacks-duncan-hodges-sadie-creese

Hunter, L.Y., Albert, C.D., Rutland, J., Topping, K. and Hennigan, C. (2024), 'Artificial intelligence and information warfare in major power states: how the US, China, and Russia are using artificial intelligence in their information warfare and influence operations', *Defense & Security Analysis*, 40(2), pp.235-269. doi: https://doi.org/10.1080/14751798.2024.2321736

Husain, A. (2021), 'AI is Shaping the Future of War', *Prism,* 9(3), pp.50-61. Available at: https://www.jstor.org/stable/48640745

Abbas. H and Ibrahim. H. (2025), 'Digital warfare: Exploring the influence of social media in propagating and counteracting hate speech in Sudan's conflict landscape', *Sudan Working Paper*, Norway: Chr Michelsen Institute, Available at: https://www.cmi.no/publications/file/9610-digital-warfare-exploring-the-influence-of-social-media-in-propagating-and-counteracting-hate.pdf

Independent. (2025), 'Why Silicon Valley is arming up with defense contracts'. Available at: https://www.independent.co.uk/tech/silicon-valley-defense-tech-boom-trump-b2847616.html [Accessed 20 October 2025]

Khamis, S. and Dogbatse, F.S. (2024), 'The Gaza war coverage: The role of social media vs. mainstream media', *IEMed: Mediterranean Yearbook*, pp. 295-300. Available at: https://www.iemed.org/wp-content/uploads/2024/09/Gaza-War-Coverage-Social-Media-Mainstream-Khamis-Sena-IEMedYearbook2024.pdf

Khanal, S., Zhang, H. and Taeihagh, A. (2025), 'Why and how is the power of Big Tech increasing in the policy process? The case of generative AI', *Policy and Society*, 44(1), pp.52-69. doi: https://doi.org/10.1093/polsoc/puae012

King, A., (2024), 'Digital targeting: Artificial intelligence, data, and military intelligence', *Journal of Global Security Studies*, *9*(2), Available at: https://academic.oup.com/jogss/article/9/2/ogae009/7667104

Keenan, T. (2001) 'Looking like Flames and Falling like Stars: Kosovo, "the First Internet War"', *Social Identities*, 7(4), pp. 539–550. doi: 10.1080/13504630120107692

Lin, P., Allhoff, F., Abney, K. (2014), 'Is Warfare the Right Frame for the Cyber Debate?', in Floridi, L. and Taddeo, M. (eds.) *The Ethics of Information Warfare. Law, Governance and Technology Series*, vol 14. Cham: Springr. doi: https://doi.org/10.1007/978-3-319-04135-3_3

Lu, Q.H.T. (2015). 'Cyber attacks: the new WMD challenge to the interagency', *InterAgency Journal*, 6(2). Available at: https://thesimonscenter.org/wp-content/uploads/2015/05/IAJ-6-2-Spring-2015-48-57.pdf

Maharani, N. (2024). 'Social media as a primary source of information: Exploring its role in disseminating the current situation in Palestine', *Gema Wiralodra*, 15(1), 275-281. doi: https://doi.org/10.31943/gw.v15i1.628

Masser, P. and Verlaan, T. (2022), 'Big Tech Goes to War: Uncovering the growing role of US and European technology firms in the military-industrial complex', *Rosa-Luxemburg-Stiftung.* Available at:https://www.rosalux.de/fileadmin/rls_uploads/pdfs/Studien/Studien_5-22_BigTech_en_web.pdf

Mazúr, J. and Patakyová, M. (2019), 'Regulatory approaches to Facebook and other social media platforms: towards platforms design accountability', *Masaryk University Journal of Law and Technology*, 13(2), pp.219-242. Available at: https://www.ceeol.com/search/article-detail?id=798066

Marigliano, R., Ng, L.H.X. and Carley, K.M. (2024), 'Analyzing digital propaganda and conflict rhetoric: a study on Russia's bot-driven campaigns and counter-narratives during the Ukraine crisis', *Social Network Analysis and Mining*, 14(1), p.170. Available at: https://link.springer.com/article/10.1007/s13278-024-01322-w

Matheson, D. and Allan, S. (2009), *Digital war reporting*, Cambridge: Polity Press.

McBride, M.K., Gold, Z. and Stricklin, K. (2020), 'Social Media Bots: Implications for Special Operations Forces', *Center for Naval Analyses.* Available at: https://apps.dtic.mil/sti/html/trecms/AD1112595/

McCarthy, J. (2007), *What is artificial intelligence?,* available at: https://cse.unl.edu/~choueiry/S09-476-876/Documents/whatisai.pdf

Miladi. N, and Milad., A. (2023), 'Digital media and the war of narratives in reporting the Palestinian-Israeli conflict' in *Global Media Coverage of the Palestinian-Israeli Conflict: Reporting the Sheikh Jarrah Evictions. London: IB Tauris*, pp.11-29.

Mueller, P. and Yadegari, B. (2012), 'The Stuxnet worm', *Département des sciences de linformatique, Université de lArizona.* Available at*: https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf*

Morris, J. (2021), 'Simulacra in the age of social media: Baudrillard as the prophet of fake news', *Journal of Communication Inquiry*, 45(4), pp.319-336/ doi: https://doi.org/10.1177/0196859920977154

Napoli, P.M. (2019), *Social media and the public interest: Media regulation in the disinformation age*, New York: Columbia university press.

Newman, N., Ross Arguedas, A., Robertson, C. T., Nielsen, R. K. & Fletcher, R., (2025), *Digital News Report 2025*. Oxford: Reuters Institute for the Study of Journalism. Available at: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2025-06/Digital_News-Report_2025.pdf

Nilsson, N.J. (1980). *Principles of artificial intelligence*. San Francisco CA: Morgan Kaufmann Publishers.

Oversight Board (2025), *Add Tools to Stop Policies Causing Information Imbalances During Conflict*. Available at: https://www.oversightboard.com/news/add-tools-to-stop-policies-causing-information-imbalances-during-conflict/?_hsenc=p2ANqtz-_wLs-4EPB0EmPGKNxRntBxe-3W7RrcxtWxit_ZNbft2zM9BXddEsDkztcMBxeeZdPpPkAlrzOHX3mYOzHspBaCmEyVkUfX9zjcr5jsZQdv5qAQJOQ&_hsmi=383284927 , [Accessed: 3 October 2025]

Pentina, I. and Tarafdar, M. (2014), 'From "information" to "knowing": Exploring the role of social media in contemporary news consumption', *Computers in human behavior*, 35, pp.211-223. doi: https://doi.org/10.1016/j.chb.2014.02.045

Rainie, L., Fox, S. and Fallows, D. (2003), *The Internet and the Iraq war*, Washington, DC: Pew Internet and American Life Project. Available at: https://www.pewresearch.org/internet/wp-content/uploads/sites/9/media/Files/Reports/2003/PIP_Iraq_War_Report.pdf.pdf

Reichert, R. (2025), 'Autonomous occupation: Israel's AI-driven drone warfare and the digital architecture of authoritarian power', *Dialogues on Digital Society*, p.29768640251381423. doi: https://doi.org/10.1177/29768640251381423

Rosa, H. (ed.), (2010), *High-speed society: Social acceleration, power, and modernity*. United States of America: Penn State Press.

Rospigliosi, A. and Raza-Mejia, S. (2021), 'Accelerated modernity: What are the social media stories undergraduate students engage with?', In *Advances in global services and retail management*, pp. 1-11, USF M3 Publishing. Available at: https://research.brighton.ac.uk/en/publications/accelerated-modernity-what-are-the-social-media-stories-undergrad/

Sætra, H.S., Coeckelbergh, M. and Danaher, J. (2022), 'The AI ethicist's dilemma: fighting Big Tech by supporting Big Tech', *AI and Ethics*, 2(1), pp.15-27. Available at: https://link.springer.com/article/10.1007/s43681-021-00123-7

Santos Okholm, C., Fard, A.E. and ten Thij, M. (2024), 'Blocking the information war? Testing the effectiveness of the EU's censorship of Russian state propaganda among the fringe communities of Western Europe', *Internet Policy Review*, 13(3), pp.1-21. Available at: https://www.econstor.eu/handle/10419/300751

Schulzke, M. (2018) 'The Politics of Attributing Blame for Cyberattacks and the Costs of Uncertainty', *Perspectives on Politics*, 16(4), pp. 954–968. doi:10.1017/S153759271800110X.

Sun, H. (2023), 'The Right to Know Social Media Algorithms', *Harvard Law & Policy Review*, 18, p.1. Available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/harlpolrv18&div=5&id=&page=

Tawil-Souri, H. and Aouragh, M. (2014), 'Intifada 3.0? Cyber colonialism and Palestinian resistance', *The Arab Studies Journal*, 22(1), pp.102-133, Available at: https://www.jstor.org/stable/24877901

The Guardian, (2025) 'Meta apologises over flood of gore, violence and dead bodies on Instagram', Available at: https://www.theguardian.com/technology/2025/feb/28/meta-apologises-over-flood-of-gore-violence-and-dead-bodies-on-instagram, [First Accessed: 03/10/2025]

USAspending.gov, (2026), 'Advanced Search', Available at: https://www.usaspending.gov/search?hash=a05a9b5ebb6bd5bf3415619c6e398594 [First Accessed: 06/03/2026]

Virilio. P, (1995), "Speed and Information: Cyberspace Alarm!,", *Le Monde Diplomatique*, Translated by Riemens. P, University of Amsterdam. Available at: https://scottkleinman.net/495dh/files/2011/09/Virilio.pdf

Willett, M. (2022), 'The Cyber Dimension of the Russia–Ukraine War', *Survival*, 64(5), pp. 7-26. doi: 10.1080/00396338.2022.2126193.

Woolley, S. and Howard, P. (2017), 'Computational propaganda worldwide: executive summary', *Computational Propaganda Project.* Available at: https://ora.ox.ac.uk/objects/uuid:d6157461-aefd-48ff-a9a9-2d93222a9bfd

Zeadally, S. and A. Flowers, (2014) 'Cyberwar: The What, When, Why, and How [Commentary]', *IEEE Technology and Society Magazine*, 33(3), pp.14-21. doi: 10.1109/MTS.2014.2345196

www.ethicalscreening.co.uk

01242 539 850

info@ethicalscreening.co.uk

www.linkedin.com/company/ethical-screening-limited

Ethical Screening is the trading name of Ethical & Environmental Screening Services Ltd.
Directors: Michael Head and Gerard Llewellyn
Registered Office: Formal House, 60 St. George's Place, Cheltenham, GL50 3PN
Registered in England & Wales.
Registration number: 3633308
VAT Registration number 713760544