BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Weaponization of data: the role of data in modern warfare

Dorcus Phanice OLASYA, Ph.D. Candidate*
Anita KIAMBA, Ph.D.**

*Department of Diplomacy and International Studies, University of Nairobi, Kenya
e-mail: dolasya@students.uonbi.ac.ke
**Department of Diplomacy and International Studies, University of Nairobi, Kenya
e-mail: akiamba@uonbi.ac.ke

Abstract

The 21st century is swamped with innumerable technologies distributed across different fields. Consequently, loads of data is being generated, transforming it into a tactical forte. Using appropriate tools and procedures, data can be appraised to generate enhanced insights into facts vital in decision-making for governments and businesses alike. However, despite its significance in strategic security, little attention has been paid to this concept. Accordingly, this article analyses ways in which data has influenced modern warfare and ways in which its potential misuse can be mitigated upon. Specifically, it highlights the aspect of power dissemination abetted by data availability, its influence in military strategies and procedures, and the role it plays in tactical intelligence and surveillance as well as military decision-making. The study adopts a qualitative and analytical research design as it comes with fewer ethical considerations. Secondary data is gathered from existing records, journals, reports, internet sources, policy papers, presented papers and books. Using the case study of Russia and Ukraine, the findings indicate that data has been transformative in present-day conflicts. Through open source data, actionable intelligence has been realized. Further, technologies such as remote sensing have been valuable to tactical intelligence, while the documentation of war crimes provided situational awareness in Ukraine as well. For ethical purposes, therefore, the use of data in the battlefield calls for sufficient regulations to oversee its use. This will also ensure caution during its deployment for the preservation of human rights as stipulated in the International Humanitarian Law.

Keywords:
data; warfare; cyber war; battlefield; military.

Article info
Received: 14 February 2025; Revised: 28 February 2025; Accepted: 5 March 2025; Available online: 2 April 2025

Citation: Olasya, D.P. and Anita Kiamba. 2025. "Weaponization of data: the role of data in modern warfare." *Bulletin of "Carol I" National Defence University*, 14(1): 90-107. https://doi.org/10.53477/2284-9378-25-06

Cyber-space, through its ability to connect the world, has been fundamental in redesigning the global security perspective. The extensive use of technology has provoked the online administration of countless businesses, hence growing the amount of data generated. In 2023, for instance, a report by Global Data projected a 26% increase in the total amount of data produced for the periods between 2017 and 2022, with mobile traffic taking up 9% of the internet traffic (Army Technology 2023). At present, approximately 8.55 billion searches are made daily using Google (Shewale 2024), and approximately 402.74 million terabytes of data are being created daily, with the figure expected to hit 181 zettabytes by the end of 2025 (Duarte 2024). Given the current emerging economic space, data has gained some sort of additional economic value. Alec Ross, a US technology-policy expert, labelled it the "raw material" of the new Industrial Revolution (Manning 2020), with other analysts referring to it as the new oil of the 21st Century, a phrase coined by the famous British mathematician and entrepreneur Clive Humby (Wilbik 2024).

As more sectors integrate technology into their daily operations, the collection of data intensifies. Just as corporate entities, Netflix for instance, have made use of data from their subscribers to understand and predict their habits (Marr 2016), governments especially in the Global South could leverage on a centralized data system (Offiong, Nta, and Etim Bassey 2021) in addition to big data generated from technologies such as the GPS systems (Nwanga et al. 2014) to combat insecurity and acts of terrorism. To note, however, is that data has the potential to be misused as was the case in Xinjiang, where the Chinese government is accused of using the IJOP app to surveil and collect data on its residents (Human Rights Watch 2019).

In the military, data can be valuable in the enhancement of situational awareness and weaponized during wars to earmark the opponents (Hammond-Errey 2022). In Liverpool for instance, during the COVID 19 pandemic in 2020, Professor Iain Buchan together with the members of the 8 Engineer Brigade, tapped into a data linkage and AI-automated intelligence system dubbed the Combined Intelligence for Population Health Action (CIPHA) to help combat the virus, classified then as a threat to the civil society (King 2024). By the same token, Ukraine, along with its allies, have made use of open source data such as satellite images to identify and attack its opponents (King 2024). With the help of a private technology company, Ukraine has benefitted immensely in the area of targeting (Farnell and Kira 2024). Data has, therefore, ceased being a mere facet in understanding the battlefield frontiers to a frontier in itself. In order to gain tactical advantage on this new characteristic of war, therefore, states require massive investment in data gathering and analysis capabilities.

Data can be described as the raw material making up any given information (Räsänen and Nyce 2013). They are recorded facts (Michael 2017) that can be logicalized and processed to come up with valuable information (Gu 2023). Data can also be viewed in terms of facts with reference to occurrences (Davenport and Prusak 1998). Herian (2021) broadly looks at it as known or supposed facts that,

if processed, could generate knowledge defining policies and also explain specific behavior. It is made up of structured and unstructured facts represented in the form of numeric, alphabets, photos, videos and audios, collected from sources such as social media, transactions, surveys just to mention but a few. It operates as a tool for dissemination in the economic process, hence crucial towards any critical decision-making process. Through data, actionable insights are realized making it an intermediary of experience and an undisputable source of truth (Herian 2021).

The use of data within the armed forces has gained traction, especially in the Global North. During the 2018 NATO Science and Technology Organization's Specialists meeting held in France, Roberto Guerrero, an official, resonated that for NATO to enhance and maximize its force, digitizing the battlefield by making use of big data is paramount (Poland 2018). Through sufficient data, Guerrero added, rational and insightful decisions on smart operations will be made. To bring this to perspective, he highlighted findings on how the inclusion of data brought about a deeper understanding of the effects of flight planning to fighters, allowing the Air Force leadership to come up with informed decisions in support of the respective operations (Poland 2018).

For the effective use of data on the battlefield, an enhanced comprehension of the problem at hand is paramount. Dawson and Matthew, therefore, propose examining it as ammunition. They argue that viewing it from this perspective will unveil its weaponry-like attributes, making it possible to understand its capabilities and enabling the defense forces to appreciate this major shift in the character of war (Dawson and Matthew 2024). Furthermore, with this concept, it will be possible to conceptualize the potential risk data poses, enlightening leaders on its threats to individuals as well as the armed forces (Dawson and Matthew 2024). To note, however, unlike physical ammunition that becomes unserviceable over a period of time, once data is stored, its value and form remain intact. Similarly, with numerous claims of data exploitation and massive violations of human rights by both state and non-state actors in the Global South, Mone et al. (2024a) propose the concept of data warfare. Data warfare in this case means the use of information and communication technologies (ICTs) by states to manipulate data systems of other states or entities for political or economic advantage (Mone et al. 2024a). This can be executed through hacking or malware attacks leading to insecurities at the national level, in addition to interfering with human rights. This concept has widely been adopted by a number of states to advance their agendas. China, for instance, has been accused by the US several times of attacking its key research facilities to steal data on its key innovations to enable its foreign influence campaigns (Farivar 2023).

As the role of data across numerous fields grows rapidly, challenges on the international legal frame to manage its malicious use have come to light. At present, the basic principles that govern personal data are being violated on purpose in favor of military operations while defying the International Humanitarian Law

(IHL) (Mone et al. 2024b). Therefore, concerns have been raised on the application of the IHL to military operations such as targeting and surveillance that majorly leverage data, considering that its operationalization is merely considered an act of espionage and hence falls under domestic rather than international law (Mone et al. 2024a). Further, due to the act of attribution, it is almost impossible for states to take responsibility for their actions. A case in point is the recent allegation of the hacking and intrusion of Kenya's key ministries and government departments by the Chinese government, allegations that have since been denied (Reuters 2023).

This article, therefore, contributes to the ongoing debate on the use of data in the modern battlefield by demonstrating its influence in the current transformation in power distributions, as well as its role in key military strategies and procedures, military decision making, in addition to tactical intelligence and surveillance. The study is anchored on two key objectives: first, to highlight the ways in which data has influenced modern warfare, and second, to discuss ways in which the potential misuse of data can be mitigated now that its incorporation in modern warfare is inevitable. The case study of the Russian - Ukraine war intends to bring to perspective the specific areas in which data has been transformative in present-day conflicts and how it has influenced major decisions on how wars are fought.

Methodology

This study seeks to highlight the role of data in modern warfare. Under the numerous activities conducted online, a lot of data is being produced. Using appropriate tools and procedures, therefore, data has been transformed to a tactical forte in key military strategies. Currently, states are not the only collectors of data; non-state actors are scrambling for its collection, analysis and exploitation to gain a niche in their respective areas. With this, data has been translated to one of the most valuable commodities not only to governments but also to non-state actors. Using the case study of the Russian – Ukrainian war, this study seeks to answer the following research questions:

1. How has data influenced modern warfare?
2. How can the potential misuse of data, especially in warfare situations, be mitigated?

The study adopts a qualitative and analytical research design as it comes with less ethical considerations while providing for the opportunity to maintain neutrality, objectivity and credibility of the data sets. Secondary data used is gathered from existing records, journals, reports, internet sources, policy papers, presented research papers and books. The findings and conclusions are drawn from the analysis of the available empirical data used.

Literature Review

Ubiquity of Data

The fourth industrial revolution is characterized by the proliferation of technologies, such as mobile phones and social media platforms, that have enhanced connectivity and communication among individuals and groups. Through these technologies, people across all divides can benefit from equal access to information and communication systems. Owing to the fact that the computing powers of cellphones today exceed organizational resources owned by institutions in the past, users, at the comfort of their cell phones, have the capabilities to access and process numerous online data sets. The processing power currently possessed by cell phones and other easily accessible devices have therefore made data ubiquitous and readily available to everyone for access and processing.

Ubiquitous data elucidates unstructured and decentralized data, sourced from different, possibly contradicting or overlapping sources (Hotho, Pedersen, and Wurst 2010), the social bookmarking systems being a typical example. Since the establishment of the social web in the late 1990s, content generated by users through the various social media sites became central to the internet culture. Through smartphones, users are able to create, upload and share content instantly from anywhere across the globe. This has created a web of interconnected networked devices, acting as information collection points publicly sharing its findings on social media. The outcome has been the proliferation of information with possible operational and intelligence value.

The accessibility of information, some of which may contain operational and intelligence value, has opened up opportunities to civilian organizations to carry out accurate intelligence analysis away from state intelligence organizations. For instance, in 2014, the covert activities of Russian soldiers in Ukraine were unfolded by the Atlantic Council and Vice News, following the combatants' activities on social media (Allen 2020). On the same note, the Global Investigative Journalism Network has been able to carry out high-caliber investigations on divergent issues by merely using readily available open-source intelligence, which is mostly generated from social media platforms (Allen 2020). Further, during the COVID-19 pandemic, using phone data, a private geospatial analytics company was able to point out the fact that several arms industries in Russia were decelerating their production, despite the government depicting very little effects of the pandemic within the country (Tucker 2020). Coincidentally, days after the report emerged, members of the forces were prohibited from carrying any digital device likely to record or store data to work (RFE/RL 2020).

Presently, content devoid of credibility is disseminated at a supersonic speed to audiences sitting in different corners of the world. Data on individual citizens and their patterns of life, likes, and preferences are easily collected, collated and analyzed by commercial

entities as well as malicious actors, using readily available tools and methodologies (Motupalli 2017). Additionally, the ubiquity of data has not only enhanced the global production chain but has also accelerated trade and investment flow. Making use of big data, companies have come up with new services, such as customer relations management, in addition to revamping their management strategies and exploring novel market domains. In a nutshell, through available data, commercial services have been transformed, directly impacting the respective economies (Ülgen 2016).

Data and Global Power Shift

For a long time, power within the international system has been discussed in the form of a state's military strength (Nye 1990). At present, however, this notion is diminishing as other factors, such as economic interdependence and the spread of technology, are diffusing power away from the traditionally great powers to private actors as well as perceived small states (Nye 2023). Additionally, along with modernization, increased communication being experienced in developing countries has also contributed to the diffusion of power from governments to private entities (Nye 2023). As information becomes powerful, the ability to respond to new information promptly becomes supreme.

Wang and Nye (2022) highlight two categories of power shifts being experienced in the current information age. First is the power shift from the west to east, that is, from Europe and the Atlantic to the Pacific and Asia, and power shifts from governments to non-governmental and transnational actors, with the second category being majorly driven by technology. Hence, power is slowly diminishing from being defined in terms of capital wealth to being defined in terms of the quantity of information one has access to (Nye 2023). With its massive cross-border distribution, therefore, information in the form of data has become a component of globalization, with data flow registering over a 100% increase between 2008 and 2020 (McCormick and Slaughter 2021).

Data is key in devising new ideas. Therefore, its unlimited flow provides economic potential because of its nonrival nature. Nonrival means that its consumption does not diminish its value, and hence it is still available for use by others (McCormick and Slaughter 2021). Because of this, innovation and, consequently, economic power depend on the quality and quantity of data accessible by states and corporations (McCormick and Slaughter 2021). Hence, tech companies, as the main collectors of data, through their newly acquired power, are taking part in foreign policies independent of their home states. A case in point is the relationship between Google and China, which contradicts American foreign policy. Further, reports have emerged of American tech companies still engaging with Huawei, completely disregarding its blacklisting by the U.S government (Apostolicas 2019).

Besides policy formulation, tech companies are rapidly investing and acquiring military technologies and capabilities that could highly impact cyber warfare.

Examining a 2018 Cybersecurity Accord, tech companies, such as Microsoft, agreed to refrain from any current or future cyber wars (Apostolicas 2019), meaning that while they do have these capabilities in place, they chose to refrain from using them. Through computer capabilities such as Quantum computing, spearheaded by private tech companies such as IBM and Intel, the current encryption methods could be unraveled. Although this is unlikely to be used in wars, it certainly would be one of the deadliest cyber-weapons globally not in the hands of government entities.

Data in Military Strategies and Decision Making

The current digital age has seen the military increasingly take advantage of data science for enhanced capabilities. By analyzing historical and real-time data, the armed forces have been able to identify trends, patterns and anomalies, thereby pointing out threats while forecasting the outcomes of upcoming military operations (Jang 2023). Through an extensive analysis of a wide range of data, it is possible to identify high-risk activities and, hence, allocate resources accordingly. Consequently, data has been able to enhance situational awareness while providing a comprehensive understanding of the operational environment, such as the weather conditions and the terrain in question (Jang 2023). Through war-gaming and simulation, available data can be used to create scenarios allowing the forces to refine their strategies. During the 2004 battle in Fallujah, for instance, war gaming was used to showcase the anticipated damage in view of classifying the reconstruction process (Mcwilliams and Schlosser 2004).

Military strategy is a critical element in military affairs, and it captures the planning phase and the execution of wars. Kofman *et al.* define military strategy as a set of guidelines states and top military officials adopt for defense and the management of war on the battlefield (Kofman et al. 2021). Through strategic decision-making, the military is able to come up with effective courses of action regarding specific situations (Zabala-López et al. 2024). This process first identifies a problem, then collects and carries out an analysis on the available data, after which the possible approach is identified, weighing its pros and cons. Depending on the specific ideologies, the decision is passed to the command and control for execution (Zabala-López et al. 2024). Military strategic decision-making is mainly carried out to deal with issues emanating from the various military domains and threatening the sovereignty and security of states.

For a successful military operation, decisions need to be prompt and accurate. Treiblmaier (2022), therefore, proposes the use of a data-driven decision-making strategy to coordinate the available resources with the goal to be achieved. He defines data-driven decision-making as the prior preparation and analysis of data for timely decision-making. Hence, this necessitates building up an analysis-based corporate culture. To build up a data-driven decision-making strategy within the military, he recommends the collection of data in all the available sources, the Internet of Things included, after which the data is evaluated, grouped and presented. This comes with

a number of advantages. For instance, with real-time data obtained from various sources, it is easy to get precise information regarding situations that can also be adjusted to meet specific undertakings. This also eliminates human biases and limitations, allowing military leaders to come up with accurate and timely decisions (Haraburda 2019). However, imaginative skills are needed to enhance the quality of decisions to be made. This strategy can be valuable in areas such as military logistics, location assessment, and deployment possibilities in addition to the replenishment of supplies and other needs on the battlefield (Treiblmaier 2022).

Similarly, to enhance military strategy, Rettore *et al.* (2023) propose the concept of Military Data Space (MDS), which integrates civilian and military data. Typically, the MDS consists of two divergent data sources: Inter- Military Data (IMD) and Extra-Military Data (EMD). While IMD encompasses data-sets provided by the military, EDM includes data-sets collected from physical or virtual sources like social media, in addition to government reports. This set of data could allow a comprehensive understanding of local behavior explaining the environment around the military operation. For efficiency, the study introduces the concept of data fusion as the authors consider that, in military applications, having varied sets of data has the potential to boost information dominance and awareness in multifaceted warfare scenarios. They add that data fusion could alleviate information overload and, therefore, enhance accuracy, coming up with sufficient knowledge to support strategic operations and situation assessment.

The study, however, notes that data harvested from external military sources do come with cyber security risks, making the military systems prone to cyber-attacks. This is well articulated by the recent rise in cyber-attacks, with reports indicating that data breaches cost businesses approximately $4.35 million in 2022, up from $4.24 million in 2021 (Griffiths 2024). It is also observed that once data is manipulated, the consequences could be severe to the populace as well as the process of military decision-making, hence undermining the integrity of the stipulated data sources. This is clearly illustrated by the current spread of misinformation and disinformation on social networking sites mostly used for political gain (Rettore et al. 2023).

Data in Tactical Intelligence and Surveillance

The Cold War, in addition to globalization, massively transformed the strategic security framework during the mid and late 1990s. However, the onset of the new millennium saw the proliferation of technologies that have not only altered every aspect of human lives but also contributed to the production of huge amounts of data globally. At present, almost 402.74 million terabytes of data are produced daily (Duarte 2024), with the figure expected to rise exponentially. Just as business entities, this massive production of real-time data has proved valuable for tactical commanders to engage successfully high-priority targets (Romine 1994). Hence, through technological inventions, the battlefield has been broadened at unimaginable levels, bringing forth the need to reevaluate the existing doctrines governing wars and conflicts.

With diverse data sources, intelligence entities have been presented with extraordinary capabilities to collect and process useful and relevant information to national interest promptly (Katz 2020). Technical intelligence, for instance, can aid the forces in uncovering signals used by the opponents and help detect abnormal behaviors within the battlefield, thus enabling them to forecast any forthcoming dangers (Katz 2020). In the Navy, data on intelligence, surveillance, and reconnaissance from devices such as drones can be useful in situational awareness or assist in safely navigating the vessels in addition to target identification (Porche et al. 2014). By the same token, through the massive data available, the armed forces have been presented with nouvelle opportunities in intelligence gathering as well as targeting domains, opening up the possibilities of swiftly unravelling a target, leading to successful litigations (King 2024). Through intrusive surveillance and targeting, a suspect's activity online, location and movement can be unraveled (Hammond-Errey 2022). This can be achieved by making use of spyware. Although Allen (2020) predicted a data-swept battlefield in 2035, where data will be supreme in all aspects, this happened sooner than expected. In 2021, the Israel Defense Forces utilized AI and data for precision to mount a series of strikes against Hamas in Gaza. Accordingly, this effective use of data prompted the attack to be labelled as the first-ever digital war (King 2024) to be successfully executed.

Currently, tactical intelligence that involves the analysis and transmission of data by specialized units and is majorly engrossed in holding up operations at the tactical level (Gragido and Pirc 2011) is already cyber-oriented. This transformation is evident in the field of open-source intelligence (OSINT), where information of tactical value is identified, processed and disseminated for tactical applications (Allen 2020). Apart from OSINT, Allen notes that the Internet of Things (IoT), because of its numerous vulnerabilities, presents exciting tactical intelligence opportunities. If intelligence and cyber operations are well harmonized, IoT could be an asset since it is capable of exposing the numerous sensors that could help unmask adversaries.

The value of data in intelligence analysis can further be showcased by its ability to highlight previously unknown relationships, even without the knowledge of the context and causality of these relations (Landon-Murray 2016). Through the analysis of data from signal intelligence sources such as phone communications, human behavior can be predicted, hence to the extreme, allowing stakeholders to devise directives to mitigate any negatives associated with the identified behavior (Reilly 2015). Additionally, considering that social media sites have been identified as the instigators of sentiment analysis, they could be of value to intelligence organizations as well as policymakers in predicting trends and, therefore, adjusting accordingly in terms of strategic change (Landon-Murray 2016). And, while data presents great opportunities for intelligence organizations, there exist possibilities of data corruption that could compromise targeting either by obstruction or leading to false targeting (King 2024). Adversaries may engineer data with the sole intent of

deceiving and confusing intelligence agencies. This manipulation could also lead to massive intelligence failure that could result in loss of lives. The October 7th 2023, attack on Israel by Hamas is a typical example, where the sensors, signals, image and human intelligence networks all failed, leading to massive loss of lives, abductions and loss of property (King 2024).

Case Study:

Russia and Ukraine

The war between Russia and Ukraine escalated on 24th February 2022, after what is described as an unprovoked and unjustified invasion of Ukraine by Russian troops (Shafy Ramadhan 2023). To date, this war has experienced a decentralized military engagement, where violence has not only been spewed over the traditional battlefields of war, that is, land, sea and air, but also through cyberspace. Making use of cutting-edge technologies, both sides have employed contemporary innovations such as armed drones and Artificial intelligence-enabled systems for prompt intelligence gathering (Favaro and Williams 2023). Leveraging the data explosion experienced globally over the past years, military intelligence, targeting and decision-making processes have been made easy and accurate (King 2024). The Russian invasion of Ukraine, therefore, presents a sneak peek of warfare in a data-rich environment, with each side capitalizing on data to foresee the enemy's next move.

Since its invasion, Ukraine, along with its allies, has been able to capitalize on technology for its defense against Russia. By making use of the current explosion of open-source data such as phone and radio messages, actionable intelligence has been realized. Through photos posted online by both civilians and combatants, locations of key Russian targets have also been identified. On December 31st 2022, for instance, exploiting pictures posted on social media by Russian soldiers, Ukraine was successfully able to strike the barracks in Mariivka, where over 600 Russian recruits are believed to have been killed (King 2024). Also, just before the invasion, open-source satellite imagery sourced from private companies, as well as photos and videos posted on social networking sites like TikTok, helped Ukraine uncover Russian forces' activities along its borders. Through social media intelligence and biometric data, it was also possible to identify Russian agents working within Ukrainian borders (Mysyshyn 2024).

Since the onset of the war, Ukraine has also made use of remote sensing for tactical intelligence. Through smart remote sensing devices, data is collected in remote areas analyzed, visualized and then interpreted using specialized software, where patterns, trends and anomalies are identified (Mysyshyn 2024). This technique has been valuable in documenting war crimes executed by the Russian troops as well as providing situational awareness on occurring events besides areas currently experiencing active war or environmental hazards. To illustrate this, although Russia

denied any dealings to do with images that occurred of dead civilians along the streets of Bucha, analysis of satellite images and videos provided placed Russian troops at the location where the bodies of the civilians were. Additionally, making use of satellite images, the cause of death of Ukrainian prisoners of war held in Olenivka in July 2022 was easily pinpointed to the Russian troops that had occupied the village (Mysyshyn 2024).

The current digital atmosphere has provided an ideal breeding ground for propaganda and disinformation, evoking the concept of weaponizing information to point out its damaging nature to the targeted group of people (Mandić and Klarić 2023). In Russia, information warfare has been used consistently as part of its strategic thinking to achieve its objectives and has continuously propagated falsified information to justify its "special military operation" in Ukraine (Fortuin 2022). Making use of social media sites, Russia has intentionally spread propaganda to garner support in addition to spreading hate against Ukraine and its Western supporting counterparts. To substantiate this, Geissler *et al.* (2023), in their study on the use of propaganda on social media during Russia's invasion of Ukraine, deduced that online propaganda has become a powerful tool in modern warfare. Making use of social media, fabricated information is easily available and can be spread swiftly. The study records that the bulk of pro-Russian messages have been disseminated through X, formerly Twitter, by bots. To note is that on the day of the UN vote on Resolution ES-11/1, Russian propaganda was directed towards the countries that abstained from voting, suggesting a deliberate and strategic manipulation of public opinion on X (Geissler et al. 2023).

Discussion and Findings:

The Russian invasion of Ukraine was majorly provoked by Ukraine's reassertion of their intentions of getting enlisted in NATO (Khoirunnisa and Sugiati 2024). Expressing its dissatisfaction, Russia deployed strategies, both military and non-military, against Ukraine with the sole intention of toppling what is seen as a Western-aligned government of Volodymyr Zelenskyy. After successfully invading and seizing Crimea in 2014, along with its strategic and economic might (Kramer 2015), Russia's expectation indicated that Ukraine would be easily subdued. However, three years on, this is not the case. Ukraine's synergy when it comes to modern technologies, along with skilled combatants, has proved valuable in the current war environment (Śliwa 2022). Following the attack, Ukraine has harnessed technology for its defense (Mysyshyn 2024), accentuating its tactical advantage and, at the same time, the numerous ethical dilemmas that come along with it. Together with private entities, Ukraine has been able to make use of data via technologies such as remote sensing, AI and facial recognition to boost its capabilities. This visible presence of non-state actors opens up new debates on the role of tech companies, mostly privately owned, manufacturing and holding patents to the numerous advanced military technologies currently being used on the battlefield.

Further, the war has transformed Ukraine into a research lab, with private companies testing and deploying their innovations on the battlefield (Sharma 2023). Tech companies such as Palantir, an American company specializing in software platforms for big data analytics, have been incorporated into the Ukrainian war routine with numerous government agencies the defense included utilizing the company's products (Bergengruen 2024). This collaboration calls to attention the extreme incorporation of technology into the various defense processes. Additionally, international companies are scrambling for data captured from the Ukrainian battlefield to help improve AI and machine learning (Sharma 2023). Consequently, a symbiotic relationship between tech companies and the state of Ukraine, both benefiting from the ongoing war, has been created and enhanced. To note further is that the relationship between the West and Ukraine has been enhanced, and this is evidenced by the bilateral agreement between the two states put forward in June 2024 (The White House 2024).

Data is the basis of innovativeness (McCormick and Slaughter 2021). Through data, the world has been able to experience new innovations such as AI and Machine Learning that have been used to alter the battlefield. Currently, the Ukrainian battlefield has encountered innovations that are likely to interfere with human judgment. Making use of the available data along with the technologies mentioned above, in the near future, key decisions on the battlefield are likely to be determined by algorithms, disregarding the human judgment, which is vital in the preservation of human rights. What this means is that there is a likelihood of massive infringement of human rights with the wide spread of the use of non-human elements within the battlefield. Additionally, as most of these technologies are owned by tech companies, the possibilities of them posing as independent actors within the battlefield are massive (Bergengruen 2024).

Nouvelle innovations have not only transformed the Ukrainian battlefield but have also presented overwhelming challenges to democracy and privacy rights (Mysyshyn 2024). Technologies in use for surveillance and face recognition, for instance, have proved to be detrimental to individuals' privacy as the majority of the time, data extracted or accessed is done without the user's consent. The use of Clearview AI, for instance, is facial recognition software identifying people by images previously sourced from social networking sites and other search engines, such as Google (Mysyshyn 2024). Although this technology is aimed at identifying Russian adversaries, the photos uploaded therein were uploaded without the consent of the users. The fact that Clearview AI's database has been sold to different authorities indicates the intentional violation of personal data for the force's gain, violating the International Humanitarian Law.

Conventional wars are regulated by the International Humanitarian Law. However, a transformed battlefield, as showcased in the Russian- Ukraine war, has uncovered loopholes in war management. The war has demonstrated that the current international institutions are not sufficient to deal with the proliferation of

data; neither are they prepared to deal with the developing flaws (McCormick and Slaughter 2021). Even with the explosion of cross-border data flows, global data management remains unregulated. This intensifies the concerns on the state of global security, bearing in mind the stipulated capabilities of data in as far as AI and machine learning are concerned. Also, as highlighted by Mone *et al.* (2024a), data inequality between the Global North and South has allowed the Global North to weaponize data to enhance their economic and technological influence. Maintaining control over data, companies in the North have continuously disregarded the opinions of those in the South on data mining and the supposed use of the data mined.

Recommendations:

The presence of data and its availability has transformed modern warfare. This is evidenced by the ongoing Russia-Ukraine war, where data has been used in war decision-making and strategies, military tactics and intelligence collection. Making use of AI and Machine learning, precision in targeting has been enhanced. And, as data is incorporated into key military strategies, concerns are raised considering that in the near future, key decisions on the battlefield are likely to be determined by algorithms, disregarding human judgment. Thus, the likelihood of contravening the International Humanitarian Law is eminent. Therefore, while technology and its accessories are deployed on the battlefield, caution needs to be exercised to ensure the preservation of human rights as per the IHL.

Additionally, the Russian- Ukraine war has demonstrated massive public – private partnership with the private sector putting forward technologies to enhance military strategies. While this is desirable, it is important to note that having these forms of technologies in the hands of private entities presents a huge challenge to global security as they can be misused if they land in the wrong hands. Also, the fact that private entities have been actively involved on the battlefield automatically grants them the chance of being players in the conflict, complicating the war situation. With this, regulations need to be put in place to manage the extent to which third parties, in this case, private entities, need to be involved in the battlefield. This will bring forth clarity on who the actual enemy is, avoiding cases of victimization, especially in as far as private entities are concerned.

Lastly, as demonstrated in this paper, the capabilities of data in war situations are massive. Basically, it has been transformed to be the "heart of the global body", as its importance cannot be overemphasized. However, despite its position, there is no international regulation managing its application and use. Consequently, chances of data misuse not only in the battlefield but also commercially do exist. Thus, just as the IHL oversees international conflicts, it is important to put in place agreeable legislation to oversee the global use of data, especially in the war front. This will ensure that ethics as well as privacy are adhered to.

Conclusion

Technology has no doubt been encompassed in every aspect of human life, and the more we use it, the more data is produced, intensifying its importance. With this, a paradigm shift has emerged across all sectors, the military included, where data has become valuable in not only intelligence gathering but also in predictive maintenance and strategic decision-making. Through massive amounts of data, military operations have been remolded to strengthen their effectiveness, thus enhancing their capabilities. Nonetheless, data has proved to be a double-edged sword; apart from generating ethical debates in matters of privacy and security, misuse of data by collecting agencies has been widely reported. With the current emerging trend of incorporating data in military operations, questions have emerged in terms of ethics, management and misuse of data within the battlefield. Based on this, therefore, this study calls for caution in the deployment of technology and its accessories on the battlefield to ensure the preservation of human rights as per the IHL. Additionally, with third parties in the form of technology companies being actively involved in the battlefield, the importance of regulations to manage their role cannot be emphasized enough, as this will eliminate instances of victimization, especially concerning these private entities. Lastly, with the rapid evolution of technology, its management, especially on the battlefield, is key. In reference to this, therefore, agreeable legislation to oversee their deployment, especially in the war front, will be valuable in ensuring ethics as far as the deployment of technology is concerned.

References

Allen, Capt T S. 2020. "Finding the Enemy on the Data-Swept Battlefield of 2035." *Military Review* 28: 28–37.

Apostolicas, Paul. 2019. "Silicon states." *Harvard International Review* 40 (4): 18–21. https://www.jstor.org/stable/26917261.

Army Technology. 2023. "How Data Became the New Frontier in Modern Warfare." https://www.army-technology.com/sponsored/how-data-became-the-new-frontier-in-modern-warfare/.

Bergengruen, Vera. 2024. "Tech Companies Turned Ukraine Into an AI War Lab." *Time.* https://time.com/6691662/ai-ukraine-war-palantir/.

Davenport, Thomas, and Laurence Prusak. 1998. *Working Knowledge: How Organizations Manage What They Know*. *Ubiquity*. Vol. 1. https://doi.org/10.1145/348772.348775.

Dawson, Jessica, and Katie E Matthew. 2024. "Data as Ammunition–A New Framework for Information Warfare." *The Cyber Defense Review* 9 (2): 93–108.

Duarte, Fabio. 2024. "Amount of Data Created Daily (2024)." *Exploding Topics*. https://explodingtopics.com/blog/data-generated-per-day.

Farivar, Masood. 2023. "FBI Warns About China Theft of US AI Technology." *Voice of America (VOA)*. https://www.voanews.com/a/fbi-warns-about-china-theft-of-us-ai-technology/7202760.html.

Farnell, Richard, and Coffey Kira. 2024. "AI's New Frontier in War Planning: How AI Agents Can Revolutionize Military Decision-Making ." *The Belfer Center for Science and International Affairs*. https://www.belfercenter.org/research-analysis/ais-new-frontier-war-planning-how-ai-agents-can-revolutionize-military-decision.

Favaro, Marina, and Heather Williams. 2023. "False Sense of Supremacy: Emerging Technologies, the War in Ukraine, and the Risk of Nuclear Escalation." *Journal for Peace and Nuclear Disarmament* 6 (1): 28–46. https://doi.org/10.1080/25751654.2023.2219437.

Fortuin, Egbert. 2022. "'Ukraine Commits Genocide on Russians': The Term 'Genocide' in Russian Propaganda." *Russian Linguistics* 46 (3): 313–47. https://doi.org/10.1007/s11185-022-09258-5.

Geissler, Dominique, Dominik Bär, Nicolas Pröllochs, and Stefan Feuerriegel. 2023. "Russian Propaganda on Social Media during the 2022 Invasion of Ukraine." *EPJ Data Sci.* 12 (1). https://doi.org/10.1140/epjds/s13688-023-00414-5.

Gragido, Will, and John Pirc. 2011. "6 - State-Sponsored Intelligence." In *Cybercrime and Espionage*, edited by Will Gragido and John Pirc, 81–114. Boston: Syngress. https://doi.org/https://doi.org/10.1016/B978-1-59749-613-1.00006-6.

Griffiths, Charles. 2024. "The Latest Cyber Crime Statistics (Updated July 2024) ." *AAG IT Support*. https://aag-it.com/the-latest-cyber-crime-statistics/.

Gu, Hongfei. 2023. "Data, Big Tech, and the New Concept of Sovereignty." *Journal of Chinese Political Science*. https://doi.org/10.1007/s11366-023-09855-1.

Hammond-Errey, Miah. 2022. "Big Data and National Security: A Guide for Australian Policymakers." Sydney: Lowly Institute. https://www.lowyinstitute.org/publications/big-data-national-security-guide-australian-policymakers.

Haraburda, Scott S. 2019. "Benefits and Pitfalls of Data-Based Military Decisionmaking." *Small Wars Journal*. https://smallwarsjournal.com/jrnl/art/benefits-and-pitfalls-data-based-military-decisionmaking.

Herian, Robert. 2021. *Data: New Trajectories in Law*. 1st edition. Routledge. https://doi.org/10.4324/9781003162001.

Hotho, Andreas, Rasmus Ulslev Pedersen, and Michael Wurst. 2010. "Ubiquitous Data" In "Ubiquitous Knowledge Discovery: Challenges, Techniques, Applications." edited by Michael May and Lorenza Saitta, 61–74. Berlin: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-16392-0_4.

Human Rights Watch. 2019. "China's Algorithms of Repression." https://www.hrw.org/sites/default/files/report_pdf/china0519_web.pdf.

Jang, Simon. 2023. "The Role of Data Collection and Big Data in Military War Planning. "| *CISS AL Big Data | Medium*. https://medium.com/ciss-al-big-data/data-is-constantly-generated-a-collected-in-the-modern-era-by-everything-3738f0d8ac10.

Katz, Brian. 2020. "The Collection Edge." *Center for Strategic and International Studies (CSIS)*. http://www.jstor.org/stable/resrep25236.

Khoirunnisa, Khoirunnisa, and Cristy Sugiati. 2024. "Cyber Warfare Strategies in the Russia-Ukraine Conflict (2021-2022): Implications for National Security and Modern Warfare." *Journal Public Policy* 10 (2): 138–45.

King, Anthony. 2024. "Digital Targeting: Artificial Intelligence, Data, and Military Intelligence." *Journal of Global Security Studies* 9 (2): ogae009. https://doi.org/10.1093/jogss/ogae009.

Kofman, Michael, Anya Fink, Dmitry Gorenburg, Mary Chesnut, Jeffrey Edmonds, Julian Waller, Kasey Stricklin, and Samuel Bendett. 2021. "Russian Military Strategy: Core Tenets and Operational Concepts."

Kramer, David J. 2015. "The Ukraine invasion: One Year Later." *World Affairs* 177 (6): 9–16. http://www.jstor.org/stable/43555264.

Landon-Murray, Michael. 2016. "Big Data and Intelligence." *Journal of Strategic Security* 9 (2): 92–121. http://www.jstor.org/stable/26466778.

Mandić, Josip, and Darijo Klarić. 2023. "Case Study of the Russian Disinformation Campaign during the War in Ukraine – Propaganda Narratives, Goals, and Impacts." *National Security and the Future* 24 (2): 97–140. https://doi.org/10.37458/NSTF.24.2.5.

Manning, Robert A. 2020. "Emerging Technologies: New Challenges to Global Stability ." https://www.internetworldstats.com/stats.htm.

Marr, Bernard. 2016. *Big Data in Practice: How 45 Successful Companies Used Big Data Analytics to Deliver Extraordinary Results*. John Wiley & Sons.

McCormick, H. David, and J. Matthew Slaughter. 2021. "Data Is Power." *Foreign Affairs.* https://www.foreignaffairs.com/articles/united-states/2021-04-16/data-power-new-rules-digital-age.

Mcwilliams, Timothy S, and Nicholas J Schlosser. 2004. "U.S. Marines in Battle: Fallujah." Marine Corps University.

Michael, David. 2017. "What and Where Is My 'Data'?" *GPSolo* 34 (2): 46–49. http://www.jstor.org/stable/26425848.

Mone, Varda, Sadikov Maksudboy Abdulajonovich, Ammar Younas, and Sailaja Petikam. 2024a. "Data Warfare and Creating a Global Legal and Regulatory Landscape: Challenges and Solutions." *International Journal of Legal Information*, 1–11.

___. 2024b. "Global Legal and Regulatory Landscape: Challenges and Solutions." *International Journal of Legal Information*, 1–11. https://doi.org/DOI: 10.1017/jli.2024.22.

Motupalli, Venkat. 2017. "How big data is changing democracy." *Journal of International Affairs* 71 (1): 71–80. https://www.jstor.org/stable/26494364.

Mysyshyn, Anna. 2024. "Advanced Technologies in the War in Ukraine: Risks for Democracy and Human Rights." *The German Marshall Fund*.

Nwanga, Mathew E., Elizabeth N. Onwuka, A.M. Albinu, and O.C. Ubadike. 2014. "Leveraging Big Data in Enhancing National Security in Nigeria." *International Journal of Knowledge, Innovation and Entrepreneurship* 2 (2): 66–80.

Nye, Joseph S. 1990. "Soft Power." *Foreign Policy*, no. 80 (March): 153–71. https://doi.org/10.2307/1148580.

___. 2023. "Soft Power" In "Soft Power and Great-Power Competition: Shifting Sands in the Balance of Power Between the United States and China.", edited by Joseph S Nye, 3–15. Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-99-0714-4_1.

Offiong, E, Eke Nta, and Inyang Etim Bassey. 2021. "The Role of Information Technology in Enhancing National Security in Nigeria (2001-2020)." *Pinisi Journal of Art, Humanity and Social Studies* 1 (1): 44–53.

Poland, Corrie. 2018. "NATO Focuses on Big Data and Artificial Intelligence ." Energy, Installations, and Environment. https://www.safie.hq.af.mil/News/Article-Display/Article/1548241/nato-focuses-on-big-data-and-artificial-intelligence/.

Porche, Isaac R, Bradley Wilson, Erin-Elizabeth Johnson, Shane Tierney, and Evan Saltzman. 2014. "Big Data:" In *Data Flood*, 1–6. Helping the Navy Address the Rising Tide of Sensor Information. RAND Corporation. http://www.jstor.org/stable/10.7249/j.ctt6wq8rr.9.

RadioFreeEurope/RadioLiberty [RFE/RL]. 2020. "Putin Bans Armed Forces Members From Carrying Electronic Devices, Gadgets." https://www.rferl.org/a/putin-bans-armed-forces-members-from-carrying-electronic-devices-gadgets/30598888.html.

Räsänen, Minna, and James M Nyce. 2013. "The Raw Is Cooked: Data in Intelligence Practice." *Science, Technology, & Human Values* 38 (5): 655–77. http://www.jstor.org/stable/23474819.

Reilly, Brant C. 2015. "Doing More with More." *American Intelligence Journal* 32 (1): 18–24. http://www.jstor.org/stable/26202099.

Rettore, Paulo H L, Philipp Zißner, Mohammed Alkhowaiter, Cliff Zou, and Peter Sevenich. 2023. "Military Data Space: Challenges, Opportunities, and Use Cases." *IEEE Communications Magazine-Series Military Communications and Networks.* https://tinyurl.com/semdam.

Reuters. 2023. "Chinese Hackers Attacked Kenya State Agencies." *The EastAfrican*. https://www.theeastafrican.co.ke/tea/news/east-africa/chinese-hackers-attack-kenya-government-4245006.

Romine, B Harl. 1994. "Intelligence data for tactical commanders." *American Intelligence Journal* 15 (1): 30–38. http://www.jstor.org/stable/44326486.

Sacks, Samm, and Justin Sherman. 2019. "Defining Data Governance." *Global Data Governance*. Concepts, Obstacles, and Prospects. New America. http://www.jstor.org/stable/resrep19968.4.

Shafy Ramadhan, Muhammad Damar. 2023. "The decision to invade: an internal perspective to the russian invasion of Ukraine." *Global: Jurnal Politik Internasional* 25 (2): 29–53. https://doi.org/10.7454/global.v25i2.1283.

Sharma, Ritu. 2023. "Ukraine-Russia War 'Attracts' Tech Firms Keen To Gather 'Invaluable' Battlefield Data & Build Future Warfare Tech." *Eurasian Times.* https://www.eurasiantimes.com/new-invaluable-data-tech-firms-want-a-piece-of-ukraines/.

Shewale, Rohit. 2024. "Google Search Statistics 2024 (Most Searches & Trends)." *Demandsage*. https://www.demandsage.com/google-search-statistics/.

Śliwa, Zdzisław. 2022. "The Synergy between Technology and Soldiers in Warfare: The Russian Armed Forces Image during the War in Ukraine." *Wiedza Obronna*.

The White House. 2024. "Bilateral Security Agreement Between the United States of America and Ukraine." 2024. https://www.whitehouse.gov/briefing-room/statements-releases/2024/06/13/bilateral-security-agreement-between-the-united-states-of-america-and-ukraine/.

Treiblmaier, Alexander. 2022. "Improving Efficiency Through Data-Driven Decision-Making In A Military Environment - ." *TDHJ*. https://tdhj.org/blog/post/data-driven-decision-making-military/.

Tucker, Patrick. 2020. "Russian Arms Production Slowed by Coronavirus, Analysts Find." *Defense One*. https://www.defenseone.com/technology/2020/05/russian-arms-production-slowed-coronavirus-analysts-find/165071/.

Ülgen, Sinan. 2016. "Data flows." *Governing cyberspace*. A Road Map for Transatlantic Leadership. Carnegie Endowment for International Peace. http://www.jstor.org/stable/resrep26924.8.

Wang, Huiyao, and Joseph S Nye. 2022. "Power Shifts in the Twenty-First Century" In "Understanding Globalization, Global Gaps, and Power Shifts in the 21st Century: CCG Global Dialogues." edited by Huiyao Wang and Lu Miao, 131–45. Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-19-3846-7_8.

Wilbik, Anna. 2024. "The Real Value of Data: A Matter of Fusion and Diffusion."

Zabala-López, Alexandra, Mario Linares-Vásquez, Sonia Haiduc, and Yezid Donoso. 2024. "A Survey of Data-Centric Technologies Supporting Decision-Making before Deploying Military Assets." *Defence Technology*. https://doi.org/10.1016/j.dt.2024.07.012.