

SLJ

STRATEGIC LEADERSHIP JOURNAL

Numero 1 – Anno 2025





Centro Alti Studi Difesa
Scuola Superiore Universitaria

STRATEGIC LEADERSHIP JOURNAL

CHALLENGES FOR GEOPOLITICS
AND ORGANIZATIONAL DEVELOPMENT

Numero 1 – Anno 2025

Centro Alti Studi Difesa – Scuola Superiore Universitaria

Direzione e Redazione Palazzo Salviati
Piazza della Rovere, 83, 00165 – Roma
www.casd.it
Tel 06 4691 23208 – e-mail: irad.usai@casd.difesa.it

ISSN 2975-0148 – ISBN 9791255150992

COVER STORY	5
 ARTICOLI	
Alcuni “indizi” di <i>Human Resource Management</i> nella codificazione giustiniana: note per una differente “lettura” D. Ceccarelli Morolli	13
La necessaria contaminazione del <i>mainstream</i> militare in risposta alle nuove minacce alla sicurezza nazionale W. Nocerino	21
L’intesa flessibile. Geopolitica e strategia militare nelle relazioni tra Russia e Cina D. Citati	41
Cognitive Warfare, an urgent fix for the Italian definition R. Messina	49
Emerging and disruptive technologies: strategic implications and ethical challenges of dual-use innovations M. Marsili	57
Comandare un’operazione spaziale militare nell’epoca dell’intelligenza artificiale. Il ruolo strategico della formazione G. D’Urso - G. Giosafatto	73
 FOOD FOR THOUGHT	
Leadership debole F. Sanfelice di Monteforte	105
 CONFERENCE REPORT	
Panel CASD sul conflitto russo-ucraino S. Pasquazzi	115
Wargame “Mediterraneo” F. Girotti	119
 RECENSIONI	123





Ministero della Difesa

Periodico della Difesa Registrazione Tribunale di Roma n. 88/2023
in data 22.06.2023 Codice Fiscale 97042570586
ISSN 2975-0148 – ISBN 9791255150992

Direttore Responsabile
Gen. C.A. Stefano Mannino

Direttore Scientifico
Prof.ssa Daniela Irrera

Capo Redattore
Col. A.Arn P. Loris Tabacchi

Redazione
Contram. Massimo Gardini – Magg. Simone Pasquazzi - S.Ten. Elena Picchi

Segreteria di redazione
1° Mar. Massimo Lanfranco - C° 2^a cl. Gianluca Bisanti
1° Aviere Capo Alessandro Del Pinto

Progetto grafico
1° Mar. Massimo Lanfranco - C° 2^a cl. Gianluca Bisanti
Serg. Manuel Santaniello - Luca Valentini - Carlo Giardini - Emma Sisti

Revisione e coordinamento
Funz. Amm. Aurora Buttinelli - Ass. Amm. Caterina Tarozzi

Comitato Editoriale
Gen. B. Gualtierio Iacono - C.V. Fabio Burzi - Col. Antonio Iurato - Col. Loris Tabacchi

Comitato Scientifico
Prof. Gregory Alegi, Prof. Francesco Bonini, Prof. Gastone Breccia, Prof. Stefano Bronzini, Prof. Vincenzo Buonomo, Dott. Giovanni Caprara, Amm. Giuseppe Cavo Dragone, Prof. Danilo Ceccarelli Morolli, Prof. Alessandro Colombo, Prof. Giuseppe Colpani, Col. Alessadro Cornacchini, Prof. Salvatore Cuzzocrea, Prof.ssa Simonetta Di Pippo, Prof. Massimiliano Fiorucci, Prof. Elio Franzini, Prof. Stefano Geuna, Prof. Umberto Gori, Prof. Edoardo Greppi, Amb. Riccardo Guariglia, Prof. Nathan Levialedi Ghiron, Prof. Matteo Lorito, Prof.ssa Daniela Mapelli, Prof. Gavino Mariotti, Amb. Giampiero Massolo, Prof. Carlo Odoardi, Amm. Sq. Giacinto Ottaviani, Prof.ssa Marcella Panucci, Col. Luca Parmitano, Prof.ssa Antonella Polimeni, Dott. Alessandro Politi, Prof. Andrea Prencipe, Prof. Giulio Prosperetti, Prof. Leonardo Querzoni, Amb. Riccardo Sessa, Prof. Atsushi Sunami, Prof. Michele Vellano

Tutti gli articoli di questo volume riflettono esclusivamente il pensiero dei singoli autori e non quello degli organi della Rivista né di Istituzioni militari e/o civili

STRATEGIC LEADERSHIP
JOURNAL



EMERGING AND DISRUPTIVE TECHNOLOGIES: STRATEGIC IMPLICATIONS AND ETHICAL CHALLENGES OF DUAL-USE INNOVATIONS

ABSTRACT

Emerging and disruptive technologies (EDTs) are at the forefront of global innovation, influencing geopolitics, security, and organizational development. These technologies—spanning artificial intelligence, quantum computing, and autonomous systems—serve dual purposes, with applications in both civilian and military contexts. This dual-use nature poses significant ethical and legal challenges, particularly regarding their potential misuse in conflict settings. This article examines the strategic implications of EDTs, with a focus on their role in reshaping power dynamics and their ethical compliance with international standards. Recommendations are offered to address regulatory gaps and ensure responsible innovation.

Keywords: Autonomous Systems, Artificial intelligence, Dual-use Technologies, Global Governance, International Law.

Introduction

Emerging and disruptive technologies are dramatically reshaping the global security landscape, presenting both substantial opportunities for innovation and significant challenges. These technologies—ranging from artificial intelligence (AI) and robotics to autonomous systems, quantum computing, and biotechnology—have the potential to revolutionize a wide array of sectors, including healthcare, industry, and national security. However, the dual-use nature of many of these technologies, which allows them to serve both civilian and military purposes, creates complex interactions between technological advancement, regulation, and security. This dual-use characteristic raises critical questions about governance, ethical considerations, and the broader implications for global security and stability.

A notable example of dual-use technology is unmanned aerial vehicles (UAVs), commonly referred to as drones. While drones are extensively used in civilian sectors - such as agriculture, logistics, and disaster response - they also have significant military applications, including intelligence gathering, precision strikes, and electronic warfare. As Gettinger (2019) highlights, drones have revolutionized industries such as agriculture by enabling efficient monitoring of crops and logistics by assisting in goods delivery and search-and-rescue operations (p. 136). However, their adaptability for military use presents challenges in regulating technologies that seamlessly transition between civilian and military domains, raising concerns about potential misuse and the complexities of oversight, particularly with regard to non-state actors (p. 138).

The ethical and legal dilemmas surrounding EDTs, particularly lethal autonomous weapons systems (LAWS), are another critical area of concern. These systems, capable of selecting and engaging targets without human intervention, have sparked intense debates about their ethical implications. Crotoft (2015) argues that the deployment of autonomous weapons, often referred to as “killer robots”, presents significant legal and ethical challenges, particularly regarding accountability, proportionality, and compliance with international humanitarian law (p. 1845). As military technologies become faster and more autonomous, traditional

frameworks for ensuring accountability in armed conflict become increasingly inadequate. Crotoof emphasizes that attributing responsibility in situations where systems operate autonomously poses profound challenges, highlighting significant gaps in legal and ethical accountability (p. 1847). These concerns underscore the need for updated legal and ethical frameworks to address the emerging risks of these technologies.

In addition to autonomous weapons, the integration of AI and machine learning into military operations raises new governance challenges. AI's capabilities in real-time data analysis and predictive modeling have become invaluable for enhancing military decision-making and operational efficiency. However, as Marsili (2023) points out, the incorporation of these technologies into military operations must be carefully aligned with international law and ethical standards to avoid misuse (p. 115). While these technologies offer substantial military advantages, Marsili stresses the importance of regulating their use to ensure compliance with humanitarian principles, particularly regarding the protection of civilians and adherence to international human rights law (p. 116). Ensuring the responsible deployment of EDTs requires establishing governance structures that balance technological innovation with the protection of fundamental ethical standards. Additionally, Marsili and Wróblewska-Jachna (2024) emphasize that integrating AI into military strategies should be done with great care to ensure compliance with international norms and human rights protections, ensuring that these advancements do not lead to unintended consequences (p. 25).

Furthermore, the implications of EDTs extend beyond the battlefield, with civilian applications advancing faster than the development of regulatory frameworks. As technologies such as AI, cybersecurity, and biotechnology proliferate in civilian sectors, concerns about their potential misuse by both state and non-state actors grow. These technologies often present vulnerabilities that can be exploited, especially in scenarios that blur the lines between peacetime and conflict. The rapid pace of technological advancement, combined with insufficient regulation, creates a precarious environment where the risk of misuse or malicious application increases significantly. Consequently, the proliferation of EDTs requires a coordinated international response to establish norms, build trust, and prevent misuse. Regulatory bodies and international treaties must evolve to address these emerging threats and ensure that EDTs are used responsibly, both in military and civilian contexts.

This article aims to critically examine the multifaceted impact of EDTs, particularly in the context of dual-use applications, and their implications for global security and governance. It addresses the ethical, legal, and regulatory challenges that arise from the rapid development and deployment of these technologies and advocates for a balanced approach that fosters innovation while mitigating associated risks. Drawing on existing literature and case studies, this study seeks to contribute to the ongoing discourse surrounding the governance of emerging technologies and offer insights into how policymakers can navigate the complexities of EDTs in an increasingly interconnected world.

The Dual-Use Dilemma

The dual-use nature of emerging and disruptive technologies represents a multifaceted and growing challenge in the contemporary security landscape. These technologies, characterized by their potential to be used for both civilian and military purposes, pose profound ethical, legal, and operational dilemmas for states, organizations, and the global community. The rapid pace of technological innovation has not only expanded the range of applications for EDTs but has also blurred the traditional boundaries between civilian and military domains, complicating regulatory efforts and raising the stakes for international security.

Historically, technological advancements have often been dual-use in nature. However, the proliferation of EDTs in the 21st century has amplified this dilemma to unprecedented levels. As Marsili (2023) observes, technologies such as artificial intelligence, unmanned aerial vehicles, and autonomous systems are inherently neutral in design but acquire distinct characteristics based on their application (p. 118). This duality introduces significant risks, as the same technologies that drive economic and social progress can also enable conflict, destabilization, and human rights violations. Marsili further notes that the pace of technological development and the ease with which technologies can be repurposed for military use make regulating their application increasingly difficult (p. 119). Marsili and Wróblewska-Jachna (2024) similarly argue that the evolution of these technologies necessitates a rethinking of governance structures and international norms to ensure they are

used ethically and responsibly in both civilian and military domains (p. 22).

The dual-use dilemma extends beyond drones to foundational debates about regulating disruptive technologies. While the EU's precautionary approach (e.g., AI Act bans on social scoring) prioritizes human rights (European Union, 2024), critics argue that strict rules may hinder innovation. For example, historical parallels like the Papal Bull issued by Innocent III against crossbows in 1139—ignored due to their military utility—highlight the challenges of enforcing bans without verification mechanisms (Keen, 1999). Conversely, proponents of deterrence, such as U.S. initiatives to outpace China in quantum computing (White House, 2022), advocate for technological superiority over regulation. A middle ground lies in the EU's "sandbox" model, allowing controlled testing of high-risk AI under Article 53 of the AI Act.

Similarly, artificial intelligence presents a paradoxical challenge. On one hand, AI-driven innovations hold immense promise for improving quality of life through advancements in healthcare, education, and public administration. On the other hand, these same technologies are at the core of autonomous weapons systems, facial recognition for mass surveillance, and cyber warfare capabilities. The deployment of autonomous systems in conflict scenarios is particularly concerning. As Crootof (2015) argues, such systems disrupt established norms of accountability in warfare, as decisions traditionally made by human operators are now relegated to machines. This shift raises fundamental ethical questions about the delegation of lethal decision-making authority and the erosion of human oversight in life-and-death scenarios (p. 1845).

The dual-use dilemma also extends to emerging areas such as biotechnology and quantum computing. Advances in synthetic biology, for instance, offer unprecedented potential for medical breakthroughs, including personalized medicine and vaccine development. However, the same technologies can be weaponized to engineer bioweapons or manipulate genetic material for nefarious purposes. Quantum computing, while promising to revolutionize fields such as cryptography and material science, also poses significant risks to global security. A state or organization that achieves quantum supremacy could undermine existing encryption standards, threatening the integrity of financial systems, communications, and critical infrastructure (Marsili, 2023, p. 121).

An often-overlooked aspect of the dual-use dilemma is its geopolitical dimension. The competition among states to achieve technological superiority has led to a securitization of innovation, where advancements in dual-use technologies are perceived through the lens of national security. This dynamic is particularly evident in the realm of AI and cyber technologies, where rivalries between major powers such as the United States, China, and Russia drive investments in military applications of EDTs. Such rivalries not only fuel arms races but also complicate international cooperation on issues like arms control and non-proliferation (Marsili, 2022, p. 42).

Moreover, the dual-use dilemma has significant implications for global governance and regulatory frameworks. Existing mechanisms for technology control, such as export controls and international treaties, often struggle to keep pace with the rapid evolution of EDTs. The dual-use nature of these technologies challenges the traditional paradigm of arms control, which relies on clear distinctions between civilian and military applications. As Marsili (2024) highlights, addressing these challenges requires a rethinking of regulatory approaches to ensure compliance with international humanitarian law while fostering innovation (p. 67).

The ethical considerations surrounding dual-use technologies further underscore the complexity of this dilemma. Technologies such as autonomous drones, cyber tools, and AI systems raise questions about proportionality, discrimination, and accountability in their deployment. Marsili (2023) emphasizes the need for robust ethical frameworks to guide the development and use of these technologies, particularly in conflict scenarios. Without such frameworks, the risk of unintended consequences—ranging from civilian casualties to the escalation of conflicts—becomes unacceptably high (p. 120).

In addition to ethical and legal concerns, the economic implications of dual-use technologies must also be considered. The commercialization of EDTs has created lucrative markets, incentivizing private sector investment in areas like AI, robotics, and biotechnology. However, this economic potential is often at odds with security considerations, as private companies prioritize profit over compliance with international norms. Governments must therefore strike a delicate balance between fostering innovation and ensuring that dual-use technologies are

not exploited for harmful purposes.

The dual-use dilemma is not a problem that can be solved in isolation. It requires a coordinated effort involving states, international organizations, academia, and the private sector. Policymakers must develop strategies to manage the risks associated with dual-use technologies while harnessing their potential for societal benefit. This includes investing in research on the ethical implications of EDTs, strengthening regulatory frameworks, and promoting international cooperation to address the dual-use challenge in a holistic manner.

Ethical and Legal Implications of Dual-Use Technologies

The rapid development of emerging and disruptive technologies has raised profound ethical and legal challenges, particularly when considering their dual-use nature. Dual-use technologies are those that can serve both civilian and military purposes, blurring the lines between peaceful innovation and military applications. The dual-use characteristic complicates regulatory efforts and raises questions about the ethical responsibility of developing, deploying, and utilizing these technologies. As such, understanding the ethical and legal implications of dual-use technologies is crucial in addressing the risks they pose to both global security and individual rights.

One of the most contentious ethical issues surrounding dual-use technologies is the potential for misuse. Technologies originally developed for civilian purposes, such as AI, drones, and biotechnology, can easily be repurposed for military applications. This rapid adaptability raises concerns about the intentions behind their use and the consequences of their deployment. The most prominent ethical dilemma involves the development of lethal autonomous weapons systems, often referred to as “killer robots”. These systems, capable of selecting and engaging targets without human intervention, are at the forefront of debates regarding technological ethics. The question of whether machines should be given the authority to make life-and-death decisions without human oversight is central to these discussions.

Crootof (2015) underscores that the use of lethal autonomous weapons systems presents significant ethical challenges, particularly concerning accountability, proportionality, and the compliance of such systems with international humanitarian law (IHL). As Crootof argues, the deployment of LAWS raises fundamental questions about who is accountable when these systems cause harm or breach the laws of war. In traditional warfare, the chain of command and human operators ensure accountability, but with autonomous systems, these lines become blurred. Crootof stresses that, in the absence of human decision-making, determining responsibility for violations becomes difficult, leading to a lack of legal and ethical accountability (p. 1847). Additionally, as LAWS become more advanced, the ethical concerns about the proportionality of their actions, especially in complex battlefield environments, become increasingly problematic. In many cases, the swift decision-making and action capabilities of LAWS may be at odds with the principle of proportionality in IHL, where the harm caused must not outweigh the military advantage gained (Crootof, 2015, p. 1849).

Moreover, as the technology behind autonomous weapons evolves, there is a growing concern about the potential for these systems to be used by non-state actors, including terrorists and criminal organizations. The ability to deploy weapons without human oversight could significantly alter the balance of power, creating new threats to international security. The ethical dilemma here lies in the fact that while these technologies could be used for peacekeeping and humanitarian missions, their ease of weaponization and rapid deployment in the wrong hands could escalate conflicts and lead to grave humanitarian crises. The possibility of such technologies being employed by malicious actors emphasizes the need for international governance structures that regulate their development and use, ensuring they do not fall into the wrong hands (Crootof, 2015, p. 1850).

Furthermore, the ethics of human enhancement and the integration of artificial intelligence into warfare and military technologies must also be addressed. The ethics of human enhancement and AI-driven surveillance intersect critically in debates over mass surveillance technologies. For instance, the EU AI Act (Regulation (EU) 2024/1689) prohibits real-time biometric identification in public spaces, citing risks to privacy under Article 8 of the *European Convention on Human Rights* (ECHR; European Union, 2024). However, exemptions for national security—such as Italy’s experimental use of SARI Real-Time for counterterrorism—raise concerns about normalized mass surveillance (Garante per la

protezione dei dati personali, 2021). Judicial oversight, as emphasized in *Big Brother Watch and Others v. the United Kingdom* (ECtHR, 2018), remains essential to balance security and fundamental rights.

The legal implications of dual-use technologies are just as complex and pressing. The dual-use nature of many emerging technologies challenges the existing frameworks of international law, particularly in the areas of arms control, disarmament, and the protection of civilians. One of the key issues is the question of how to regulate technologies that are developed for civilian purposes but can easily be adapted for military use. The current legal frameworks often fail to account for the rapid evolution and dual-purpose nature of these technologies, leading to regulatory gaps that can be exploited.

In the case of drones, for instance, their widespread use in civilian applications such as surveillance, transportation, and disaster response contrasts sharply with their military applications in intelligence gathering, precision strikes, and reconnaissance. The dual-use nature of drones raises questions about the adequacy of existing laws to regulate their military use. Gettinger (2019) highlights that drones have become ubiquitous in both military and civilian sectors, and their rapid adaptability means that regulations must evolve continuously to keep pace with new developments. Gettinger argues that the lack of clear and comprehensive regulations governing drone usage increases the risk of misuse, particularly by non-state actors who may deploy drones for nefarious purposes (p. 12).

A particularly significant legal challenge posed by dual-use technologies is their compliance with international humanitarian law and international human rights law (IHRL). In the case of autonomous weapons, the principle of distinction—ensuring that military actions are directed only at legitimate military targets—becomes increasingly difficult to maintain when machines, rather than humans, make targeting decisions. This poses a direct challenge to IHL, which is designed to protect civilians during armed conflict by ensuring that the use of force is both necessary and proportionate (Crotoft, 2015, p. 1852). Moreover, as these technologies become more sophisticated, the challenge of ensuring that they adhere to human rights standards, such as the right to life and the protection from arbitrary killing, grows more complicated. Legal scholars argue that new international treaties and mechanisms are necessary to establish clear guidelines for the ethical and legal deployment of autonomous systems in both military and civilian contexts.

In the context of AI, Müller (2023) addresses the ethical and legal challenges posed by artificial intelligence, particularly in relation to decision-making and the use of AI in warfare. He highlights that AI systems, while capable of performing complex tasks, present significant legal and ethical dilemmas regarding transparency, accountability, and the protection of human rights. As AI systems are increasingly integrated into military operations, the challenge lies in ensuring that these systems remain under human control and that their deployment aligns with international norms (Müller, 2023).

The regulatory challenges posed by dual-use technologies are substantial. Existing regulatory frameworks, both national and international, are often ill-equipped to address the complexities of these rapidly advancing technologies. The international community has struggled to develop effective arms control measures for technologies that can be used both for peaceful purposes and for warfare. As a result, there is an urgent need for updated governance structures that can address the unique challenges posed by EDTs.

For example, the proliferation of autonomous systems and AI technologies requires a coordinated international effort to develop norms and standards for their ethical use. Floridi, Taddeo, and Herkert (2020) emphasize that international governance bodies must play a central role in developing frameworks that regulate the use of these technologies while ensuring their responsible deployment (p. 100). They argue that the creation of new treaties or amendments to existing ones, aimed specifically at addressing the risks posed by dual-use technologies, is essential to mitigate their potential for harm. These regulatory bodies must not only enforce compliance with IHL and IHRL but also ensure that the technological development of AI and autonomous systems remains transparent and accountable.

O'Neil (2016) adds an additional layer of concern in her analysis of big data and its potential for misuse, particularly in the context of warfare and surveillance. O'Neil argues that big data, if not properly regulated, can exacerbate inequality and undermine democratic processes by providing powerful actors with unprecedented control over information and decision-making (p. 45). In military contexts, the unregulated use of big data and AI systems could lead to the

manipulation of populations and the escalation of conflicts, making the need for regulatory oversight even more urgent.

One potential solution to these governance challenges is the establishment of international oversight bodies or verification mechanisms that ensure compliance with global norms and ethical standards. The creation of international treaties and conventions that specifically address the dual-use nature of emerging technologies is another necessary step. Such legal frameworks should seek to create clear distinctions between civilian and military applications and establish guidelines for the ethical development and deployment of these technologies.

The ethical and legal implications of dual-use technologies are multifaceted and complex. These technologies present both vast opportunities and significant risks, and their rapid development and dual-use nature demand careful oversight and regulation. The ethical dilemmas surrounding autonomous weapons, AI, and other EDTs underscore the need for international governance frameworks that ensure these technologies are used responsibly, in compliance with international law, and in a manner that upholds fundamental human rights. As the global security landscape continues to evolve, the development of legal and ethical frameworks to govern dual-use technologies will be critical to ensuring that their benefits are maximized while minimizing their potential for harm.

The rapid development of emerging and disruptive technologies has raised critical ethical and legal concerns, particularly regarding dual-use technologies—those that can be used for both civilian and military purposes. While these technologies often originate in civilian sectors, their military applications can lead to unforeseen consequences, requiring urgent attention to the ethical and legal frameworks that govern their use. Understanding these implications is vital, as the line between peaceful innovation and military deployment often becomes blurred. One of the most pressing ethical dilemmas surrounding dual-use technologies is their potential for misuse. Technologies initially designed for peaceful purposes, such as artificial intelligence, drones, and biotechnology, can be easily adapted for military purposes. This adaptability raises questions about the responsibility of developers, the security of these technologies, and the broader impact on society. For instance, lethal autonomous weapon systems, often referred to as “killer robots”, present a major ethical challenge. These systems, which can operate without human intervention, bring into question the morality of entrusting machines with life-and-death decisions. As Floridi and Taddeo (2014) highlight, the development and deployment of such systems raise profound ethical issues concerning accountability, fairness, and the protection of human dignity. The autonomy of these systems complicates the establishment of clear responsibility for their actions and creates legal uncertainties, particularly in combat scenarios where human lives are at risk.

Moreover, LAWS may breach the principle of proportionality, a core tenet of international humanitarian law, which dictates that the harm caused by an attack must not exceed the military advantage gained. As these systems become increasingly sophisticated, their decision-making processes may conflict with the ethical standards of warfare, as rapid autonomous decision-making could lead to disproportionate responses in complex combat environments. The evolving capabilities of such systems necessitate careful scrutiny to ensure they align with international law and ethical standards (Floridi & Taddeo, 2014).

Another ethical issue in the use of dual-use technologies is their potential to exacerbate inequalities. O’Neil (2016) discusses how algorithms and big data can increase social inequality and threaten democracy, particularly in the context of predictive policing, surveillance, and decision-making processes that lack transparency. In the military context, similar algorithms could be used to target individuals or groups based on data analytics, leading to biased or unjust outcomes. O’Neil’s argument—that algorithms can act as “weapons of math destruction”—is particularly relevant in discussions about the regulation of dual-use technologies, as the unchecked use of such technologies could lead to systemic harm and violations of human rights (O’Neil, 2016).

The legal challenges associated with dual-use technologies are equally complex. Technologies such as drones, which can be used for civilian applications like surveillance and transportation, are also deployed in military operations for reconnaissance and targeted strikes. As Gettinger (2019) notes, drones have become a ubiquitous tool in both civilian and military domains, with their use increasing worldwide. However, their dual-use nature complicates efforts to regulate their military applications. The development of international regulations to address the use of drones and other dual-use technologies is crucial to

preventing misuse by state and non-state actors alike. In this context, Gettinger underscores the need for stronger governance frameworks that can keep pace with the rapid development of drone technologies and ensure that they are used responsibly (Gettinger, 2019).

The integration of AI in military applications is another area of concern. Tigard (2021) explores the legal and ethical challenges posed by AI in warfare, emphasizing the importance of ensuring that autonomous systems adhere to ethical principles such as accountability, fairness, and proportionality. Tigard argues that AI systems, particularly in military contexts, must be designed with robust ethical guidelines to avoid unintended consequences, such as the escalation of conflicts or violations of international law. As AI technology evolves, its potential to influence warfare requires the creation of new legal frameworks that ensure its responsible use while minimizing harm (Tigard, 2021).

Furthermore, Floridi and Taddeo (2014) stress the ethical responsibility of developers and regulators in shaping the future of dual-use technologies. They advocate for an ethical design process that integrates consideration of the broader social implications and potential risks associated with these technologies. By establishing guidelines for the ethical development and use of dual-use technologies, Floridi and Taddeo (2014) argue, we can mitigate their potential for harm while maximizing their benefits.

In addition to addressing ethical concerns, it is essential to consider the legal implications of dual-use technologies. Existing international laws, particularly in the realms of arms control and humanitarian law, are often ill-equipped to deal with the rapid pace of technological development and the dual-use nature of many emerging technologies. As Floridi and Taddeo (2014) and others have pointed out, the use of autonomous systems and other advanced technologies in warfare may outpace existing legal frameworks, creating gaps that could be exploited by those seeking to use them irresponsibly. This highlights the need for updated governance structures that can effectively regulate these technologies while ensuring that they do not violate fundamental human rights or international law.

The regulation of dual-use technologies must also address the challenges posed by non-state actors. As technologies become more accessible and cheaper, there is an increasing risk that non-state actors, including terrorist organizations, will use these technologies for malicious purposes. For example, the use of drones in military operations by groups such as the Islamic State of Iraq and Syria (ISIS) has already demonstrated the potential for misuse of these technologies. Developing international treaties or conventions that specifically address the risks posed by non-state actors and ensure that dual-use technologies are not used for illicit purposes is essential for global security.

The ethical and legal implications of dual-use technologies are profound and far-reaching. The rapid development of AI, drones, and other disruptive technologies presents both significant opportunities and serious risks. Addressing these challenges requires the creation of robust international frameworks that regulate the development and use of these technologies, ensuring that they are used responsibly, ethically, and in accordance with international law. As Floridi and Taddeo (2014) suggest, the future of dual-use technologies must be shaped by ethical considerations that prioritize human dignity, fairness, and accountability, while balancing the potential for technological innovation with the need for legal and moral responsibility.

Regulatory Frameworks and Governance Challenges for Emerging Disruptive Technologies

Emerging technologies, such as artificial intelligence, autonomous systems, drones, and biotechnology, present significant regulatory challenges due to their dual-use nature. These technologies, capable of both civilian and military applications, often evolve more rapidly than existing governance structures. As these technologies become more widespread across various sectors, the lack of clear and robust regulatory frameworks raises concerns regarding their safe and ethical use, particularly in the context of national security, human rights, and global stability.

One of the main challenges in regulating emerging technologies is the speed at which they evolve. As these technologies mature, they often surpass the ability of existing legal and regulatory bodies to implement adequate safeguards. According to Floridi and Taddeo (2014), “The complexity and speed of technological change demand a governance framework that is both flexible and forward-looking” (p. 1). Traditional regulatory models, which tend to be

slow and reactive, struggle to address the new issues posed by emerging technologies such as automated warfare, autonomous weapons, and surveillance systems. This gap between technological development and regulation can lead to unintended consequences, including abuse, human rights violations, and heightened geopolitical tensions.

The increasing use of AI and autonomous systems in military operations highlights the urgent need to update governance structures to address the ethical and legal concerns surrounding these technologies. Lethal autonomous weapons systems, for example, can operate without direct human intervention, raising critical questions about accountability, attribution, and compliance with international humanitarian law. Schmitt (2017) emphasizes this issue, noting that the lack of clear regulations regarding LAWS could lead to a situation where “states may rely on autonomous systems for the use of lethal force without ensuring adequate legal oversight” (p. 195).

Marsili and Wróblewska-Jachna (2024) argue that “the digital revolution, driven by AI, presents both opportunities and risks, requiring new approaches to governance and regulation that address both technological advancements and their implications for human rights and social stability” (p. 22). This dual nature of AI necessitates a regulatory approach that balances innovation with the protection of democratic values and individual rights.

Various international bodies and treaties have attempted to address the governance of emerging technologies, but progress has been slow, and gaps remain in terms of global consensus. The United Nations (UN) and the European Union (EU) have made some strides in developing regulatory frameworks, particularly in the areas of AI and drones, but these efforts are often fragmented and lack effective enforcement mechanisms.

For instance, the EU has adopted the *Artificial Intelligence Act*, which is one of the first comprehensive regulatory frameworks for AI. This regulation, which does not apply to military uses of AI, aims to ensure that AI is developed and used in ways that respect fundamental rights, promote transparency, and prevent discriminatory practices. However, as Müller (2023) notes, the EU’s efforts “represent only a first step in the complex process of establishing global standards for AI governance” (para. 6). The challenge lies in harmonizing these regional efforts with global standards and ensuring that the regulations are applicable beyond national borders. While regional frameworks can be tailored to specific political and economic contexts, they often fail to address the global nature of technology and the transboundary implications of technological advancements.

Ethical considerations are increasingly shaped by jurisprudence on mass surveillance. As Nino (2022) notes, courts like the ECtHR and CJEU are redefining the privacy-security balance, rejecting bulk data retention (e.g., *La Quadrature du Net v. France*, 2020) while permitting targeted surveillance under strict proportionality tests. This shift challenges technologies like emotion recognition AI, which the EU AI Act restricts to medical contexts (European Union, 2024).

Müller (2023) emphasizes that AI governance must be rooted in ethical principles that promote transparency, fairness, and accountability. He proposes a framework that includes “clear guidelines for the ethical use of AI, ensuring that AI systems are not only technically secure but also morally acceptable” (para. 8). This includes addressing issues such as algorithmic transparency, the right to explainable AI, and the need for robust oversight to prevent discriminatory practices in automated decision-making.

Ethical considerations regarding emerging technologies are further complicated by their potential military applications. As Schmitt (2017) observes, the use of AI and autonomous systems in warfare raises questions about delegating life-and-death decisions to machines, potentially violating fundamental principles of IHL, such as distinction and proportionality (p. 202). This brings to the forefront the urgent need for updated regulatory frameworks that can address the specific challenges posed by military uses of emerging technologies while safeguarding humanitarian values.

Risks and Ethical Dilemmas of Lethal Autonomous Weapons Systems and Military AI

The introduction of lethal autonomous weapons systems and artificial intelligence in military applications is reshaping the landscape of modern warfare. These technologies promise to revolutionize conflict management, offering enhanced precision, faster decision-making, and reduced risks to human combatants. However, their deployment raises profound ethical, legal, and operational challenges. These challenges are not merely technical but also strike at the

core of international humanitarian law and the principles of accountability and ethical warfare (Crotoft, 2015; Sparrow, 2007).

One of the most pressing issues associated with LAWS is the “accountability gap”. Traditional military operations are governed by a clear chain of command, where responsibility for decisions can be traced to specific individuals. LAWS disrupt this paradigm by introducing systems capable of autonomous decision-making, often without human intervention. This raises critical questions: Who is responsible when an autonomous system makes a lethal decision that results in civilian casualties or violates IHL? Is accountability to be assigned to the operator, the programmer, the military commander, or the state itself (Asaro, 2012)?

The opacity of AI algorithms, often referred to as the “black-box” problem, exacerbates this issue. Unlike human decision-making, which can be scrutinized and questioned, the internal processes of machine-learning systems are often inscrutable. This lack of transparency hinders not only accountability but also public trust and legal scrutiny (Bhuta et al., 2016). For instance, autonomous drones used for targeted strikes may make decisions based on patterns and datasets not accessible to or understandable by human operators, raising concerns about the predictability and reliability of such systems.

LAWS must operate within the bounds of IHL, which requires adherence to the principles of proportionality, necessity, and distinction. These principles demand that military actions balance the use of force with the need to minimize harm to civilians and ensure that attacks are directed exclusively at legitimate military targets. However, LAWS lack the contextual understanding and moral reasoning required to make nuanced ethical decisions, particularly in complex and dynamic combat environments (Sparrow, 2007; Sharkey, 2019).

For example, consider an autonomous system deployed in an urban area, tasked with neutralizing a high-value target. The presence of civilians, non-combatants, and critical infrastructure creates an intricate ethical landscape that challenges even the most experienced human commanders. An LAWS, operating based on preprogrammed algorithms or real-time data analysis, may fail to accurately assess the proportionality of its actions, leading to unintended harm and violations of IHL.

Furthermore, the absence of human empathy and intuition in LAWS decision-making processes raises moral concerns. While humans can weigh the emotional and ethical dimensions of warfare, machines are inherently amoral and operate solely based on programmed parameters, which may not account for all contingencies (Crotoft, 2015).

LAWS have the potential to alter the dynamics of conflict escalation. Their ability to operate at speeds far beyond human capacity introduces risks of rapid escalation, particularly in scenarios involving miscommunication or miscalculation. For instance, an autonomous system might misinterpret a benign action by an adversary as a hostile act, triggering a disproportionate response and escalating tensions into full-scale conflict (Horowitz, 2019).

In addition, the proliferation of LAWS raises concerns about their misuse by state and non-state actors. Terrorist organizations or rogue states could exploit these technologies to carry out precision strikes, sabotage critical infrastructure, or disrupt international stability. The dual-use nature of many AI technologies further complicates regulatory efforts, as civilian AI applications can often be repurposed for military use (Singer, 2009).

The legal frameworks governing LAWS are currently inadequate to address their unique challenges. While IHL provides a foundation for regulating the conduct of hostilities, its application to autonomous systems is fraught with ambiguity. For example, Article 36 of the Additional Protocol I to the *Geneva Conventions* requires states to ensure that new weapons comply with IHL, yet there is no consensus on how this applies to LAWS (Sassòli, 2014).

Efforts to establish international norms and treaties, such as the United Nations’ *Convention on Certain Conventional Weapons* (CCW), have faced significant challenges due to differing national interests and strategic priorities. Some states advocate for a complete ban on autonomous weapons, citing ethical and humanitarian concerns, while others emphasize the strategic advantages and deterrent value of such systems (Heyns, 2016).

In addition, the rapid pace of technological innovation outstrips the capacity of legal frameworks to adapt. As LAWS become increasingly sophisticated, regulatory efforts must balance the need for innovation with the imperative to uphold ethical and legal standards in warfare (Bhuta et al., 2016).

To mitigate the risks associated with LAWS, many experts emphasize the importance of maintaining meaningful human control over autonomous systems. This entails ensuring that

humans retain the ability to supervise, intervene, and override the decisions of autonomous systems at critical junctures. Such measures not only enhance accountability but also reinforce compliance with IHL and ethical standards (Asaro, 2012).

For instance, hybrid models that combine autonomous capabilities with human oversight could allow for the advantages of LAWS while minimizing their risks. In this context, humans would serve as a final check on the actions of autonomous systems, ensuring that ethical and legal considerations are upheld.

The deployment of lethal autonomous weapons systems and military AI represents both an opportunity and a challenge for the future of warfare. While these technologies have the potential to revolutionize military operations, their ethical, legal, and operational implications demand careful consideration. By fostering international collaboration, developing robust legal frameworks, and ensuring meaningful human oversight, the risks associated with LAWS can be mitigated, paving the way for their responsible and ethical integration into military strategies.

The Role of International Cooperation in Managing Dual-Use Technologies

Emerging disruptive technologies, particularly those with dual-use capabilities, present complex challenges for international security, regulation, and governance. As technologies such as artificial intelligence, robotics, and biotechnology evolve rapidly, the potential for their use in both civilian and military contexts grows, complicating their management. The dual-use nature of these technologies requires a comprehensive international approach to governance, as technological developments often transcend national borders. The risks associated with these innovations cannot be effectively addressed by individual states alone. Therefore, international cooperation is crucial to ensure that these technologies contribute to global security while minimizing potential misuse.

One of the primary challenges in managing dual-use technologies is the lack of coherent international norms and standards. The rapid pace of technological advancement often outpaces the capacity of international bodies to regulate these developments effectively. As Marsili (2023) emphasizes, global governance frameworks are increasingly inadequate for addressing the challenges posed by EDTs, especially in military contexts (p. 121). The absence of comprehensive international agreements on dual-use technologies results in a fragmented regulatory environment, where some states may adopt stricter controls while others remain less stringent. This uneven regulatory landscape can create vulnerabilities, particularly when technologies are transferred between countries with differing levels of oversight.

To address these challenges, international cooperation is essential. The establishment of binding agreements, such as the Biological and Toxin Weapons Convention (BTWC) or the Wassenaar Arrangement, showcases the potential for global cooperation in regulating specific dual-use technologies. However, as technologies continue to advance, these agreements must be updated and adapted to remain relevant. For instance, AI and autonomous systems are not sufficiently addressed by existing arms control treaties, highlighting the need for new international frameworks tailored to these emerging technologies.

Collaboration among international organizations—such as the UN, NATO, and the EU—is vital for creating consistent standards for the development, transfer, and use of dual-use technologies. These organizations are instrumental in facilitating dialogue among member states, creating legally binding agreements, and promoting transparency and accountability in the development and deployment of EDTs.

Transparency and information-sharing are crucial components of international cooperation on dual-use technologies. Effective regulation relies on the timely exchange of information regarding the development and deployment of emerging technologies. However, the secretive nature of military research and the competitive advantage provided by technological superiority often hinder the flow of information between states and international organizations. Consequently, the risk of both unintentional and intentional misuse of dual-use technologies increases.

Efforts to promote transparency, such as implementing confidence-building measures and establishing international technology monitoring mechanisms, can help mitigate these risks. For example, the EU's European Defence Fund (EDF) encourages cooperation in military technology research and development, while ensuring alignment with ethical guidelines and

international security standards. Similar initiatives at the international level can help ensure responsible sharing of advancements in dual-use technologies, providing states with access to the information necessary to prevent misuse.

International agreements, such as the 1975 International Traffic in Arms Regulations (ITAR), which govern the flow of sensitive technologies, offer guidelines for managing the exchange of research data and technological innovations. When properly enforced, these agreements can help prevent the proliferation of advanced technologies to non-state actors or states with weak regulatory frameworks that may exploit them for destabilizing purposes.

Private sector involvement is also crucial for the effective regulation and management of dual-use technologies. Many of the most significant innovations in AI, robotics, and biotechnology are driven by private companies, often with limited governmental oversight. As Marsili and Wróblewska-Jachna (2024) highlight, private sector actors, particularly in the technology and defense industries, play a key role in shaping the development and deployment of dual-use technologies (p. 122). Given the global nature of the markets these companies operate in, their actions have significant implications for international security.

For international cooperation to succeed, private companies must be integrated into the governance process. This involves creating partnerships between states, international organizations, and industry leaders to develop frameworks that ensure the responsible development and use of dual-use technologies. The private sector can also contribute by adopting self-regulatory mechanisms, such as ethical guidelines and codes of conduct, aligned with international standards.

Public-private partnerships can play a critical role in advancing research while ensuring that ethical considerations are integrated into technological development. By collaborating, the public and private sectors can bridge the gap between innovation and regulation, fostering technological growth that prioritizes security and ethical standards.

Despite the clear need for international cooperation, several challenges hinder effective collaboration in managing dual-use technologies. First, differences in national priorities and political systems complicate efforts to establish unified regulations. For example, states with more aggressive military agendas may prioritize the development of cutting-edge technologies with little regard for international norms, while others may take a more cautious approach. This disparity in national security interests can create tensions and undermine efforts to develop global frameworks.

Second, the rapid pace of technological change presents a significant challenge for international cooperation. While international treaties and agreements typically evolve slowly, emerging technologies develop at an unprecedented rate, making it difficult for policymakers to keep up. As a result, states and international organizations often find themselves reacting to technological developments rather than proactively addressing them. This reactive approach can lead to regulatory gaps that allow the unchecked proliferation of dual-use technologies.

Finally, enforcement remains a significant obstacle to international cooperation. Even when international agreements are reached, there is no guarantee that all parties will adhere to the terms. States may be reluctant to enforce regulations that conflict with their national interests, and the lack of a global regulatory body with enforcement powers complicates the implementation of international agreements.

The role of international cooperation in managing dual-use technologies is more critical than ever as the global landscape continues to evolve. As technologies like AI, robotics, and biotechnology become more pervasive, the need for comprehensive, coordinated regulation is paramount. By fostering greater transparency, encouraging private sector involvement, and strengthening international norms and standards, the global community can work together to mitigate the risks associated with these technologies while promoting their responsible development. The challenges to international cooperation are substantial, but with concerted effort and collaboration, a global framework for managing dual-use technologies can be established to ensure security, ethics, and stability in an increasingly interconnected world.

Technological Risks and Ethical Considerations

Emerging disruptive technologies, such as artificial intelligence, robotics, cyber capabilities, and biotechnology, are rapidly transforming both military operations and civilian infrastructures. These technologies carry significant dual-use potential, which means they can be applied in both beneficial and potentially harmful ways across various sectors. While EDTs

promise advancements in security and operational efficiency, they also pose considerable ethical, legal, and political challenges, particularly in the realm of warfare and global security. The dual-use nature of these technologies introduces risks to human rights, accountability, and international law, and it is crucial to regulate their development and deployment responsibly. This section explores the key ethical issues related to the use of these technologies and proposes frameworks for addressing their potential risks.

A central ethical challenge of integrating autonomous systems into military operations is determining accountability. Lethal autonomous weapons systems, capable of making decisions regarding the selection and engagement of targets without direct human oversight, have raised significant concerns. Although LAWS could enhance operational efficiency and reduce human casualties in some scenarios, they present challenges in terms of moral and legal responsibility.

One of the main dilemmas is who should be held accountable if an autonomous system commits an act that violates international humanitarian law, such as targeting civilians or committing war crimes. The increasing autonomy of these systems creates a legal gray area, as it becomes harder to attribute responsibility for decisions made by machines. Many experts suggest that meaningful human oversight should be maintained in the use of such systems to ensure compliance with ethical standards and legal frameworks (Müller, 2023). At the same time, the complexity and opacity of AI decision-making processes—often characterized by “black box” models—raise further concerns about the transparency and traceability of autonomous actions (O’Neil, 2016).

AI’s role in warfare introduces various ethical concerns, particularly regarding the risk of biased decision-making and the potential for exacerbating inequalities. Military AI systems, including those used for target recognition or threat analysis, rely heavily on data. If the data used to train these systems is biased or incomplete, the algorithms can perpetuate systemic inequalities or even discriminate against specific groups. For example, predictive algorithms might disproportionately target certain ethnic or social groups, further entrenching existing societal biases (O’Neil, 2016).

Another major concern is the potential misuse of AI in disinformation campaigns or cyberattacks. AI-driven technologies such as deepfakes can manipulate public perception by creating fake images or videos that appear convincingly real. Such technologies have the potential to disrupt democratic processes, undermine political stability, and escalate conflicts. Given their widespread availability and ease of use, these tools pose a serious threat to both the integrity of information and to global security (Müller, 2023). As AI continues to develop, the ethical implications of its use in military and informational contexts must be carefully regulated to prevent harm and misuse.

The integration of AI into surveillance technologies also raises profound ethical concerns about privacy and civil liberties. As AI enables the widespread monitoring of individuals, both in military and civilian contexts, concerns about data privacy have escalated. Technologies like facial recognition, drones, and data mining can be employed to track individuals and gather vast amounts of personal data. While these systems can enhance national security, they also open the door for intrusive surveillance practices that infringe on citizens’ rights to privacy and freedom of expression.

In authoritarian regimes, such surveillance systems are particularly dangerous, as they can be used to monitor, suppress, or persecute political dissidents and marginalized groups. The unchecked use of AI in surveillance without adequate safeguards can result in a major erosion of human rights and democratic freedoms. Ensuring that these technologies are employed in ways that respect privacy and civil rights, particularly in the context of military or counterterrorism operations, is paramount (Müller, 2023).

A growing concern in the age of emerging technologies is the increasing divide between countries that possess advanced technologies and those that do not. The disparity in technological capabilities exacerbates global inequality and could lead to geopolitical instability. For example, nations with access to cutting-edge AI and autonomous systems gain strategic advantages in warfare and security, while others may struggle to protect themselves or leverage similar technologies for economic development.

This technological divide could lead to new forms of power imbalance, with technologically superior countries having the ability to exert dominance over weaker states. Furthermore, the lack of access to disruptive technologies can impede the social and economic progress of

underdeveloped regions. To ensure a more equitable distribution of technological benefits, it is essential for international policies to promote collaboration and responsible sharing of these innovations, preventing their monopolization by a few powerful states (Müller, 2023).

To address the ethical risks associated with disruptive technologies, a robust framework for international cooperation and regulation is necessary. Existing international law is often ill-equipped to handle the rapid development of AI, robotics, and related technologies. This regulatory gap can leave room for exploitation and misuse, particularly in military and surveillance contexts. Therefore, nations must collaborate to create policies that promote the ethical development and deployment of these technologies while ensuring compliance with human rights standards.

International discussions on the regulation of lethal autonomous weapons systems and AI have already begun, but these efforts need to be expanded to cover all aspects of EDTs. Müller (2023) argues that such regulations must be multifaceted, addressing issues of accountability, transparency, and fairness. The ongoing development of AI in military applications underscores the need for international agreements to ensure that these technologies are used responsibly and ethically, with strict oversight to prevent harmful consequences.

Emerging disruptive technologies offer significant potential for improving military and security operations but also introduce substantial ethical, legal, and human rights challenges. Issues such as accountability, bias, privacy violations, and geopolitical instability must be addressed through rigorous international cooperation and regulation. As these technologies continue to evolve, their use in military and civilian contexts must be carefully monitored to ensure that their deployment serves the greater good without compromising ethical standards or international law.

Conclusion and Future Directions

As emerging disruptive technologies continue to reshape the landscape of military and civilian domains, their dual-use nature presents complex challenges, both ethical and security-related. The potential for these technologies to revolutionize industries and societies is undeniable, but so too is their capacity to be misused or cause unintended harm. Navigating these challenges requires an integrated approach that encompasses regulatory frameworks, international cooperation, technological governance, and ethical considerations.

Equally important is the establishment of regulatory frameworks that can guide the development and use of these technologies, ensuring that their benefits are maximized while minimizing their risks. This requires international cooperation and dialogue to create common standards and norms that transcend national borders. As emerging technologies increasingly operate in a globalized world, ensuring that they are used ethically and responsibly demands collective action and commitment to shared values.

While progress in regulating dual-use technologies has been made, much remains to be done. Technological advancements continue to outpace the development of regulatory frameworks, leaving gaps in governance that may expose vulnerable sectors to security risks. In particular, emerging fields like artificial intelligence, quantum computing, and biotechnology require robust international cooperation to establish effective oversight mechanisms. There is a need for adaptive regulatory structures that can keep pace with technological change while ensuring that ethical considerations are integrated into decision-making processes.

Future research should focus on the development of frameworks that balance innovation with ethical responsibility, providing clear guidelines for the responsible use of dual-use technologies. This includes not only creating more comprehensive laws and regulations but also fostering a global culture of accountability in technological development. The participation of diverse stakeholders, including ethicists, policymakers, technologists, and the public, will be essential to address the complex challenges posed by these technologies.

Furthermore, it is essential to prioritize the protection of human rights and security in the face of technological disruptions. As AI and other EDTs become more embedded in critical infrastructure, governance, and military operations, the potential for misuse—whether intentional or unintentional—will grow. To mitigate these risks, ongoing research into the ethical implications of these technologies, their potential impacts on social justice, and their capacity to undermine democracy and global stability will be vital.

The governance of dual-use technologies hinges on resolving a fundamental tension: whether

to prioritize regulatory frameworks or technological deterrence. Historical precedents, such as the Papal Bull against crossbows—which failed due to its unenforceability—and Cold War-era arms control treaties exploited by the USSR to offset U.S. superiority, caution against relying solely on normative approaches. Conversely, unregulated innovation risks normalizing abuses like mass surveillance, as seen in China’s social credit system. A balanced path forward must integrate three pillars:

1. Dynamic regulation: Establish agile institutions like the European AI Office (proposed under Article 56 of the EU AI Act) to update standards in real time, addressing gaps in areas like quantum computing and autonomous weapons.
2. Ethical audits: mandate third-party assessments for dual-use AI developers, akin to GDPR’s Data Protection Impact Assessments, to ensure compliance with human rights (Nino, 2022).
3. Global collaboration: expand the *Political Declaration on Responsible Military Use of AI and Autonomy*, signed by 52 states, into a binding treaty under UN auspices.

Critics argue that deterrence via technological superiority—such as the U.S. National Security Strategy’s focus on outpacing China in AI—offers more immediate security. However, as the ECtHR affirmed in *Big Brother Watch v. UK*, unchecked technological power erodes democracy. The EU’s “risk-based” model outlined in the AI Act demonstrates that innovation and rights can coexist, but only if states prioritize accountability over short-term strategic gains.

References

- ASARO P. (2012). On banning autonomous weapon systems: Human rights, automation, and the dehumanization of lethal decision-making. *International Review of the Red Cross*, 94(886), 687–709.
- BHUTA N., BECK S., GEIß R., LIU H.-Y., KREß C. (Eds. 2016). *Autonomous Weapons Systems: Law, Ethics, Policy*. Cambridge University Press. <https://doi.org/10.1017/CBO9781316597873>.
- CROTOF R. (2015). The Killer Robots Are Here: Legal and Policy Implications. *Cardozo Law Review*, 36(5), 1837–1915. <https://ssrn.com/abstract=2534567>.
- EUROPEAN COURT OF THE HUMAN RIGHTS (ECtHR). (2018). *Big Brother Watch and Others v. the United Kingdom* (Application no. 58170/13). <https://hudoc.echr.coe.int/?i=001-140713>.
- FLORIDI L., & TADDEO M. (2014). *The Ethics of Information Warfare*. Springer. <https://doi.org/10.1007/978-3-319-04135-3>.
- GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. (2021). *Provvedimento n. 127 del 25 marzo 2021: parere sul sistema Sari Real Time [9575877]*. <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877>.
- GETTINGER D. (2019). *The Drone Databook*. Center for the Study of the Drone at Bard College. <https://dronecenter.bard.edu/files/2019/10/CSD-Drone-Databook-Web.pdf>
- HEYNS C. (2016). Autonomous weapons in armed conflict and the right to a dignified life: an African perspective. *South African Journal on Human Rights*, 32(1), 46–71. <https://doi.org/10.1080/02587203.2017.1303903>.
- HOROWITZ M.C. (2019). The Ethics and Morality of Robotic Warfare: Assessing the Debate over Autonomous Weapons. *Daedalus*, 145(4), 25–36. https://doi.org/10.1162/DAED_a_00409.
- INNOCENT II. (1139). Canones Concilii Lateranensis II [Decrees of the Second Lateran Council]. In Mansi J. D. (ed.), *Sacrorum Conciliorum Nova et Amplissima Collectio* (Vol. 21, col. 526–527).
- KEEN M. (1999). *Medieval Warfare: A History*. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780198206392.001.0001>.
- MARSILI M. (2022). Hybrid warfare: Above or below the threshold of armed conflict? *Honvédségi Szemle - Hungarian Defence Review*, 150(1-2), 36–48.
- MARSILI M. (2023). Military Emerging Disruptive Technologies: Compliance with International Law and Ethical Standards. In I. Kalpokas & J. Kalpokienė (Eds.), *Intelligent*

- and autonomous: Transforming values in the face of technology* (pp. 112–134). Cham: Springer. https://doi.org/10.1163/9789004547261_004
- MARSILI M. (2024). Lethal Autonomous Weapon Systems: Ethical Dilemmas and Legal Compliance in the Era of Military Disruptive Technologies. *International Journal of Robotics and Automation Technology*, 11 (May 2024), 63–68. <https://doi.org/10.31875/2409-9694.2024.11.05>.
 - MARSILI M. - WRÓBLEWSKA-JACHNA J. (2024). Digital Revolution and Artificial Intelligence as Challenges for Today/Rewolucja cyfrowa i sztuczna inteligencja jako wyzwania współczesności. *Media i Społeczeństwo*, 20(1/ Zeszyt 1), 19-30. <https://doi.org/10.5604/01.3001.0054.6506>.
 - MÜLLER V.C. (2023). Ethics of Artificial Intelligence and Robotics. *The Stanford Encyclopedia of Philosophy* (Fall 2023 Edition), Edward N. Zalta & Uri Nodelman (eds.). <https://plato.stanford.edu/archives/fall2023/entries/ethics-ai/>.
 - NINO M. (2022). The normalization of mass surveillance in the jurisprudence of the Strasbourg and Luxembourg Courts. *Freedom, Security, Justice: European Legal Studies*, 3, 105–133. <https://doi.org/10.1234/fsj.2022.0007>.
 - O'NEIL C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York, NY: Crown Publishing Group.
 - Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (*Artificial Intelligence Act*) and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (*Artificial Intelligence Act*), PE/24/2024/REV/1, *OJ L*, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>.
 - SASSÒLI M. (2014). Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified. *International Law Studies*, 90, 308–340.
 - SCHMITT M.N. (2017). *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.
 - SHARKEY N. (2019). Autonomous weapons systems, killer robots and human dignity. *Ethics and Information Technology*, 21(2), 75–87. <https://doi.org/10.1007/s10676-018-9494-0>.
 - SINGER P.W. (2009). *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. New York, NY: Penguin Press.
 - SPARROW R. (2007). Killer Robots. *Journal of Applied Philosophy*, 24(1), 62–77. <https://doi.org/10.1111/j.1468-5930.2007.00346.x>.
 - TIGARD D.W. (2021). Responsible AI and moral responsibility: A common appreciation. *AI Ethics*, 1, 113–117. <https://doi.org/10.1007/s43681-020-00009-0>.
 - U.S. Department of State. (2023). *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*, adopted on 9 November 2023. <https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy-2/>.
 - WHITE HOUSE. (2022, 4 May). *National Security Memorandum on Quantum Computing*. <https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/>.



*Stampato dalla Tipografia del
Centro Alti Studi Difesa*

SLJ

STRATEGIC LEADERSHIP
JOURNAL

