**Regulatory Challenges of Military Technology Transfer in the Age of AI**

**Dissertation Proposal supervised by**

**Prof. Niva Elkin Koren and Prof. Assaf Hamdani**

**May Har-Shai**

**אתגרים אסדרתיים של העברת טכנולוגיות צבאיות בעידן הבינה המלאכותית**

**הצעת מחקר לדוקטורט בהנחיית פרופ' ניבה אלקין-קורן ופרופ' אסף חמדני**

**מאי הר-שי**

Contents

[Introduction 4](#_Toc198542850)

[Chapter 1: Military Tech-Transfer 7](#_Toc198542851)

[1. Military Tech-Transfer Dynamics 7](#_Toc198542852)

[2. Regulatory Framework 10](#_Toc198542853)

[Chapter 2: Military Tech-Transfer in the Age of AI 28](#_Toc198542854)

[3. Technological Characteristics of AI 28](#_Toc198542855)

[4. Military AI Ecosystem 33](#_Toc198542856)

[5. Interim Conclusions 43](#_Toc198542857)

[Chapter 3: Tech-Transfer Regulatory Challenges in the Age of AI 45](#_Toc198542858)

[6. Facial Recognition Technology: Case Study 45](#_Toc198542859)

[7. Regulatory Gaps 51](#_Toc198542860)

[8. Conclusion 57](#_Toc198542861)

[Research Question 58](#_Toc198542862)

# Introduction

This research proposal addresses a central question: **To what extent, and in what ways, should existing regulatory frameworks governing military tech-transfer be adapted to meet the unique challenges posed by the AI era?**

Historically, military tech-transfer followed two primary dynamics: the repurposing of military innovations for civilian use, and the adaptation of civilian technologies for military purposes.[[1]](#footnote-2) This proposal contends that the advent of AI has introduced a novel dimension—the erosion of clear boundaries between civilian and military uses, and the intensification of interdependence between the two domains.[[2]](#footnote-3)

This blurring of lines is driven by two key factors, both examined in detail in the proposed research: (1) the unique technological characteristics of AI systems; and (2) an innovation ecosystem shaped by reliance on civilian infrastructure and data, alongside evolving geopolitical and economic incentives that promote cross-sector collaboration.[[3]](#footnote-4)

AI systems rely heavily on access to vast and diverse datasets. The performance of machine learning (ML) algorithms is directly tied to the quantity and variety of data used in training.[[4]](#footnote-5) As a result, strict separation between civilian and military datasets can impair innovation and reduce system performance. Moreover, AI is dynamic in nature. Unlike static technologies, AI systems evolve continuously by ingesting new data—regardless of origin—leading to “black box” models with unclear decision-making processes. In such systems, determining whether an output derives from military or civilian data could be challenging.[[5]](#footnote-6)

Beyond these technological features, shifting strategic and economic interests further entangle civilian and military innovation. The characteristics of AI influence not only the technologies themselves but also the broader ecosystem in which they are developed. Geopolitical dynamics—such as the global AI arms race—shape regulation and incentivize state involvement in innovation. Governments increasingly rely on cooperation with private firms, particularly Big Tech companies,[[6]](#footnote-7) for critical resources such as access to data (the “fuel” of AI), cloud infrastructure, strategic investments in startups, and the adaptation of commercial technologies for military use.[[7]](#footnote-8)

Private companies, driven in part by the need to access large, varied datasets, are increasingly engaging in military initiatives—often without direct compensation. This trend is especially visible in recent conflicts, such as those in Israel and Ukraine, where companies have provided AI-based battlefield tools and infrastructure. These engagements allow firms to test, refine, and validate their technologies in real-time, boosting the commercial value of their products across both defense and civilian markets.[[8]](#footnote-9)

Traditional regulatory frameworks for military tech-transfer were developed with conventional dual-use technologies in mind and assumed a clear separation between civilian and military domains.[[9]](#footnote-10) Historically, their core objective has been to balance innovation with the imperative of national security.[[10]](#footnote-11) In the context of AI, however, this separation no longer holds. The unique attributes of AI systems and the evolving structure of the innovation ecosystem create regulatory gaps and legal challenges that are not adequately addressed by existing frameworks—necessitating targeted adjustments..[[11]](#footnote-12)

This proposal is structured into three chapters:

**Chapter One** explores the current landscape of military tech-transfer. It outlines the underlying dynamics and examines existing regulatory frameworks, including their objectives. It also considers emerging shifts in regulatory goals prompted by the rise of AI and surveys various global regulatory models, suggesting that their distinctions may likewise become less meaningful in the AI era.

**Chapter Two** presents the core premise of this research: that advancements in AI have fundamentally transformed the dynamics of military tech-transfer. It examines the key drivers of this shift, with particular emphasis on the technological characteristics of AI and an innovation ecosystem shaped by geopolitical forces.

**Chapter Three** analyzes the regulatory challenges that result from these developments. A case study on facial recognition technology (FRT) illustrates the convergence of military and civilian AI applications and the legal ambiguities that arise. The chapter then identifies broader structural and doctrinal gaps in current frameworks, driven by AI’s distinct characteristics and development context.

Ultimately, this proposed research aims to lay the groundwork for a normative and doctrinal analysis of how legal systems must evolve to govern AI-driven military tech-transfer in a world where the boundary between military and civilian domains is increasingly blurred—and the interdependence between them is only growing.

# Chapter 1: Military Tech-Transfer

To assess the impact of AI development on the military tech-transfer regulatory framework, it's important to first understand the current landscape. This chapter will define tech-transfer and its key dynamics, followed by a review of existing regulations. It will discuss objectives related to military tech-transfer, focusing on innovation and national security risks, as well as recent geopolitical concerns. Furthermore, it will categorize regulatory tools that promote innovation and those that mitigate security risks and examine global regulatory approaches to military innovation.

## Military Tech-Transfer Dynamics

Tech-transfer, or spillover,[[12]](#footnote-13) refers to the movement of technology between entities such as companies, governments, and academic institutions, or to its adaptation for new purposes.[[13]](#footnote-14) This research proposal focuses specifically on the transfer of military technologies, with an emphasis on the interactions between military institutions and commercial companies.

Military tech-transfer involves the diffusion and dual-use application of innovations across civilian and defense domains.[[14]](#footnote-15) This concept highlights the central roles of both state actors and private industry in advancing military innovation. Understanding these interactions is essential to assessing how tech-transfer contributes to national defense capabilities.[[15]](#footnote-16)

Military tech-transfer primarily occurs primarily through two key dynamics: Spin-Off and Spin-On. Spin-Off refers to the adaptation of military technologies for civilian applications,[[16]](#footnote-17) while Spin-On involves the incorporation of civilian innovations into military systems.[[17]](#footnote-18) Historically, both processes have followed relatively linear, unidirectional paths, shaped by technological developments during the Industrial Revolution and periods of armed conflict. [[18]](#footnote-19)

Technology encompasses not only physical artifacts but also the theoretical knowledge that underpins them.[[19]](#footnote-20) While many technologies have dual-use potential, most work funded by government agencies or private companies is designed for specific purposes.[[20]](#footnote-21) Private companies focus on innovation for business goals, while government agencies promote it to fulfill public missions like national defense.[[21]](#footnote-22)

During the first three Industrial Revolutions, military R&D has been a significant driver of innovation.[[22]](#footnote-23) Military innovations were then spun off to the commercial sphere.[[23]](#footnote-24) A notable example of spin-off technology is the Internet, whose earliest version, ARPANET, was developed with critical funding from the American Department of Defense (DoD).[[24]](#footnote-25) Other examples include civilian space systems;[[25]](#footnote-26) The Global Positioning System (GPS) was initially designed to calculate launch-point routes for ballistic missiles;[[26]](#footnote-27) and civilian drones,[[27]](#footnote-28)

World War II marked a pivotal moment in civil-military cooperation, establishing robust defense industries capable of supporting large-scale militaries.[[28]](#footnote-29) By the late 20th century, the focus shifted from Spin-Off to Spin-On, meaning military innovation increasingly relied on commercial technology advancements, particularly information technology. [[29]](#footnote-30) The Spin-On phenomenon refers to transferring technologies, processes, or innovations developed in the civilian sector to the military. [[30]](#footnote-31) This transfer includes technological innovations, human resources, manufacturing processes, and management techniques initially created commercially.[[31]](#footnote-32)

Spin-On is often viewed as a method for integrating cutting-edge commercial technologies that are currently unavailable to defense systems due to either commercial or governmental barriers.[[32]](#footnote-33) For example, commercial jet engines have been adapted for military aircraft, and large commercial aircraft have been modified for military roles such as transport and aerial tanking.[[33]](#footnote-34) In some cases, militaries modify commercial technologies and ideas or utilize the same equipment.[[34]](#footnote-35)

The current regulatory framework governing military tech-transfers was established in response to the dynamics discussed in this subchapter. The following subchapter will analyze this existing regulatory framework, outline its objectives, present examples of various regulatory tools, and explore different models and approaches to regulating military innovation.

## Regulatory Framework

The previous subchapter explored the concept of military Tech-transfer, emphasizing the long-standing reliance between the military sector and the private commercial sector regarding military innovation. Historically, this dependence has been one-sided, with clear distinctions between various applications. This subchapter will examine the regulatory framework that has been developed to address the current dynamics of military tech-transfer.

### Regulation Objectives

Regulation functions as a mechanism of governance by shaping the behavior of actors through the imposition, establishment, monitoring, and enforcement of legal rules.[[35]](#footnote-36) Governments possess diverse regulatory tools designed to respond to the complex and evolving needs of citizens, communities, and national economies.[[36]](#footnote-37) Within the academic literature on military tech-transfer, regulation is generally understood to serve two principal objectives: promoting technological innovation while mitigating security-related risks, particularly those arising from the potential misuse of advanced technologies.[[37]](#footnote-38)

Technological advances have introduced a new objective that military tech-transfer regulations must address: economic security, often called "geoeconomic" concerns.[[38]](#footnote-39) The term “geoeconomic” describes the interconnected nature of economics and security in the international trade and investment law framework.[[39]](#footnote-40) It highlights how economic gains can impact security, raises awareness of the security risks associated with economic interdependence and digital connectivity, and reflects the intense competition over technological development.[[40]](#footnote-41)

The tools utilized to achieve this objective share similarities with those found in national security, including the promotion of innovation and efforts to minimize the risks of technology leakage to hostile entities. However, the underlying purpose differs. Consequently, there is an increasing need to foster innovation, and the definition of what constitutes a hostile entity may change over time.

### Regulatory Tools

After outlining the primary objectives underlying the regulatory framework governing military tech-transfer, the following subchapter will present illustrative examples of regulatory tools, categorized according to the two overarching functions discussed above: **promotive regulation**, which facilitates innovation and collaboration, and **restrictive regulation**, which aims to mitigate risks by controlling the dissemination of sensitive military information and technologies.

#### Promotive Regulation

This subchapter explores the regulatory tools and legal frameworks that facilitate private-sector innovation in defense technology and tech-transfer, including IP laws, financial subsidies, and related mechanisms. While numerous measures are in place to encourage innovation within the public sector, the focus is specifically on those designed to support and promote private-sector contributions.

##### Intellectual Property (IP)

IP rights allow abstract knowledge to be transformed into a tangible asset under a legal framework that governs ownership and usage rights.[[41]](#footnote-42) This enables knowledge transfer across research sectors by selling and licensing IP rights between the private and defense sectors.[[42]](#footnote-43) IP rights, such as patents, copyrights, and trade secrets, aim to incentivize innovation by allowing firms to capture a larger share of the social returns to their research investments.[[43]](#footnote-44)

Patent law incentivizes the disclosure of technological inventions by granting an exclusive development period.[[44]](#footnote-45) This encourages the sharing of valuable information that might otherwise remain secret.[[45]](#footnote-46) While public disclosure offers recognized advantages, it also comes with certain risks, as it makes information about the invention accessible globally to both allies and adversaries.[[46]](#footnote-47)

In the defense context, oversight of patent disclosure is essential to prevent sensitive innovations from benefiting adversaries.[[47]](#footnote-48) For example, both the British Patents Act and the European Patent Office allow governments to restrict patent processing for national security reasons.[[48]](#footnote-49)

Scholars have proposed various strategies by which governments can leverage patent policy to advance national security objectives. Stowsky argues that states seeking to limit foreign involvement in critical technology—or to control the global dissemination of domestic knowledge—must adopt a proactive stance.[[49]](#footnote-50) This may include engaging foreign scientists and manufacturers as research sponsors or as premium-paying customers for specialized applications, thereby steering technological development while protecting strategic interests.[[50]](#footnote-51)

In his article on war and IP, Yu highlights how nations often seek to prevent their patent systems from benefiting adversaries during armed conflict. He notes that patents held by enemy states can obstruct innovation critical to wartime efforts, underscoring the broader dilemma of balancing IP protections with the imperative to prevent the misuse or withholding of essential technologies.[[51]](#footnote-52)

Bloomfield offers a complementary perspective, emphasizing the dual nature of IP. While patent and trade secret laws allow private entities to safeguard and monetize their innovations, governments can also use IP classifications to regulate and restrict access to technical data, which is considered a security risk. Bloomfield describes this as the exercise of "anti-property" powers—where IP laws serve as tools to delineate the boundary between privately held information and data subject to national security control.[[52]](#footnote-53)

One historical example of this approach is the US’s actions during World War I, where patents held by German IP rights holders were confiscated to neutralize any potential advantage they could provide to the enemy. This demonstrates how states can suspend or revoke IP rights as a measure to safeguard national security in times of conflict.[[53]](#footnote-54)

While patents are intended to promote innovation, research suggests that they are insufficient on their own; competition is also a critical driver. Aghion’s study on European firms found that patent protection, by itself, had “no effect on R&D intensity.” However, following major competition reforms, countries with strong patent regimes saw greater innovation compared to those with weaker protections. [[54]](#footnote-55) This indicates that patents are most effective when complemented by robust market competition. Conversely, excessive protection that suppresses competition may hinder technological progress and should therefore be applied with caution.[[55]](#footnote-56)

Licensing arrangements allow the receiving state to access technology and legal authorization in exchange for financial or other considerations. These agreements often include clauses restricting the re-export of licensed equipment.[[56]](#footnote-57) Historically, licensing agreements have facilitated the production of military equipment abroad, enabling joint ventures or external production while maintaining control over the technology's distribution and use.[[57]](#footnote-58)

Trade secret laws are a vital component of IP protection, particularly for safeguarding technological elements such as source code, algorithms, and proprietary solutions—provided they remain confidential and retain independent commercial value.[[58]](#footnote-59) Unlike patents or copyrights, trade secrets do not require formal registration or public disclosure, offering businesses greater flexibility.[[59]](#footnote-60) However, their protections are limited, as they are vulnerable to reverse engineering and unauthorized disclosure.[[60]](#footnote-61)

Despite these limitations, trade secret laws are widely utilized in industries like software development, where they help firms protect commercially valuable information and sustain competitive advantage.[[61]](#footnote-62) Nevertheless, the assertion of trade secrecy can generate tension between private vendors and public institutions, particularly when transparency and accountability are at stake.[[62]](#footnote-63) A notable example involves the New York Police Department, which invoked Palantir’s trade secrecy rights to resist disclosing information in response to public records requests under New York’s Freedom of Information Law. This case underscores how trade secrecy claims can complicate efforts to balance corporate confidentiality with the public’s right to information.[[63]](#footnote-64)

##### Finance Subsidies

Government policies can foster innovation through various mechanisms, including prizes for inventions, research grants, and tax subsidies.[[64]](#footnote-65) In the US, direct federal funding plays a substantial role in annual R&D expenditures, particularly through grants and investments in national laboratories.[[65]](#footnote-66) Additionally, the government incentivizes research through tax credits and provisions allowing businesses to deduct research and experimental expenses.[[66]](#footnote-67) Although prizes currently represent a smaller portion of this framework, their role in encouraging innovation is steadily increasing.[[67]](#footnote-68)

A prominent example of financial subsidies driving technological innovation is the CHIPS Act of 2022, which established the *Creating Helpful Incentives to Produce Semiconductors (CHIPS) for America Fund*. This multi-billion-dollar initiative seeks to revitalize domestic semiconductor manufacturing by providing direct subsidies, tax benefits, and research investments.[[68]](#footnote-69) Its goal is to reduce reliance on foreign supply chains and stimulate private-sector investment in critical technologies.[[69]](#footnote-70)

Another tool for promoting military innovation involves U.S. military assistance to allies, often tied to domestic purchasing requirements under Off-Shore Procurement.[[70]](#footnote-71) For example, U.S. aid to Israel has enabled Israeli companies to open subsidiaries licensed to operate within the U.S. These entities facilitate defense contracts with the U.S. military and participation in joint aid-financed programs, strengthening bilateral defense ties.[[71]](#footnote-72) This model illustrates how financial subsidies can strategically foster both domestic and international innovation while reinforcing key defense partnerships.

#### Restrictive Regulation

Following the discussion of regulatory tools that promote innovation and tech-transfer, this subchapter shifts focus to oversight mechanisms aimed at addressing the security risks posed by technological advancement.[[72]](#footnote-73) As innovation introduces new vulnerabilities, regulatory regimes must evolve to mitigate emerging threats.[[73]](#footnote-74) In this domain, the state holds primary responsibility, uniquely positioned to safeguard the public interest and national security.[[74]](#footnote-75)

In the context of military tech-transfer, a core objective of risk regulation is to prevent the proliferation of sensitive technologies to hostile states or non-state actors. Another key goal is managing the risks posed by dual-use technologies, which may serve both civilian and military purposes. Regulatory mechanisms are essential to ensuring that civilian-developed technologies are not repurposed in ways that threaten security or violate international legal norms.[[75]](#footnote-76) They also play a crucial role in facilitating compliance with non-proliferation agreements, reinforcing a state’s commitment to global stability and security cooperation.[[76]](#footnote-77)

##### Secrecy Orders

Governments may impose secrecy orders to protect sensitive military technologies, prohibiting inventors from disclosing or publishing certain inventions without prior authorization. In the U.S., the *Invention Secrecy Act of 1951* authorizes federal agencies to assess whether public disclosure of a patent application might pose national security risks.[[77]](#footnote-78) If so, the Commissioner of Patents may issue a secrecy order, classifying the invention and withholding publication.[[78]](#footnote-79) Applicants are also prohibited from filing related patents in foreign jurisdictions for at least six months. These orders remain in effect as long as national security concerns persist.[[79]](#footnote-80)

Secrecy orders significantly limit a patent applicant’s ability to secure international protection, requiring prior government approval for any foreign filings.[[80]](#footnote-81) Unauthorized disclosure can result in severe penalties, including the abandonment of the U.S. patent application. These measures underscore the extent to which states act to safeguard sensitive technological assets.[[81]](#footnote-82)

In the UK, Section 22 of *the British Patents Act* similarly allows the registrar to block the publication of applications that could endanger national security. The registrar must inform patent holders of any restrictions and, unless contrary to the public interest, provide regular updates.[[82]](#footnote-83) The law also invalidates licensing agreements that restrict public-use rights, reinforcing the principle that public interest overrides private contractual limitations.[[83]](#footnote-84)

##### Local Control Regulation

Banning foreign software is one method the U.S. government uses to address national security risks posed by foreign-controlled technologies. In August 2020, President Trump issued an executive order under the International Emergency Economic Powers Act (IEEPA) prohibiting American citizens from conducting business with ByteDance Ltd., the Chinese parent company of TikTok.[[84]](#footnote-85) In 2021, President Biden rescinded this order and replaced it with a new one reiterating national security concerns. It classified China as a “foreign adversary” posing threats to U.S. security, foreign policy, and economic interests through control over software platforms.[[85]](#footnote-86)

These executive actions laid the foundation for broader legislative measures. In 2024, Congress passed the *Protecting Americans’ Data from Foreign Adversaries Act* (The Act), which formalized U.S. efforts to counter risks from foreign-controlled digital technologies.[[86]](#footnote-87) Section 2§(g)(1) of the Act defines “foreign adversary countries” to include China, Russia, Iran, and North Korea and identifies ByteDance as a “Foreign Adversary Controlled Application.”[[87]](#footnote-88) The Act grants the President authority to impose targeted, flexible restrictions in response to evolving national security threats.[[88]](#footnote-89)

Following its enactment, ByteDance challenged the law in court. However, in December 2024, the U.S. Court of Appeals for the D.C. Circuit upheld the Act, affirming its constitutionality. The court ordered TikTok to divest its U.S. assets to a non-Chinese entity within 90 days or face a complete operational ban.[[89]](#footnote-90) This decision demonstrated judicial alignment with legislative and executive efforts to mitigate foreign technology risks.

During divestment negotiations, ByteDance encountered new regulatory barriers from the Chinese government, which imposed national security restrictions on the export of algorithms, effectively preventing the transfer of TikTok’s engineering operations outside China.[[90]](#footnote-91)

Beyond software bans, the U.S. also exercises authority over foreign acquisitions through the *Committee on Foreign Investment in the United States (CFIUS)*.[[91]](#footnote-92) CFIUS reviews transactions involving foreign entities that may pose national security risks, particularly in sectors involving sensitive technologies or intelligence capabilities. If unresolved concerns persist, the committee may recommend that the President block the acquisition to protect national interests.[[92]](#footnote-93)

##### Export Control Regulation

Export control regimes are national legal mechanisms that restrict the outbound transfer of military-use and dual-use goods and technologies based on national security concerns.[[93]](#footnote-94) Since World War II, countries—particularly the U.S. and European nations—have used such regimes to align trade practices with defense priorities, limit proliferation, and restrict the military capabilities of adversarial states.[[94]](#footnote-95) As international relationships have changed post-Cold War, the national security concerns that have guided export controls have also undergone policy changes that reflect the changing concerns of the countries.[[95]](#footnote-96)

Whang, in *Trade and Emerging Technologies*, argues that economic objectives have increasingly merged with national security strategies. U.S. export controls on dual-use goods now serve not only to mitigate security risks but also to maintain global technological leadership.[[96]](#footnote-97)

While export controls cover a range of sectors, this analysis focuses on regulations concerning software acquisition. Fideler identifies two regulatory approaches: market regulation, which restricts developers and sellers, and use regulation, which targets buyers and end-users. Recently, regulation has shifted toward seller-side controls, including license requirements and distribution limitations. Fideler categorizes controls into item-based (technology type), user-based (end-user identity), and use-based (intended application).[[97]](#footnote-98)

The Wassenaar Arrangement (WA) serves as the foremost international mechanism for coordinating export controls. This multilateral framework establishes guidelines for the export of dual-use goods and military items, including advanced surveillance software.[[98]](#footnote-99) The ‘cyber’ amendments to WA adopted during the 2010s served as the foundation for subsequent dual-use export reforms worldwide.[[99]](#footnote-100) This influence extended to major players such as the US, China, and the EU, who have assumed leading roles in the production, sales, and governance of cyber-surveillance technology.[[100]](#footnote-101)

The WA includes a "control list" that categorizes items with military or dual-use applications, offering member states a basis for aligning their domestic export control policies.[[101]](#footnote-102) Non-member states like China often reference the WA control list when shaping their export regulations, demonstrating its broader influence.[[102]](#footnote-103)

The EU has developed its dual-use export controls through Regulation (EU) 2021/821, incorporating elements of the WA control list. [[103]](#footnote-104) This regulation governs technologies that have both civilian and military applications, including cyber-surveillance tools.[[104]](#footnote-105) While member states can implement dual-use export controls, they must ensure these measures align with overarching EU regulations to maintain consistency across the bloc.[[105]](#footnote-106)

In the US, two principal frameworks govern export controls: the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR).[[106]](#footnote-107) Administered by the State Department, ITAR focuses on defense-related goods and services, requiring licenses for their export and re-export.[[107]](#footnote-108) The EAR, managed by the Department of Commerce, oversees dual-use technologies listed on the Commerce Control List (CCL) and mandates licensing requirements for specific items based on their potential applications.[[108]](#footnote-109) Additionally, the US employs the Vulnerabilities Equities Process (VEP), which outlines procedures for determining whether government-discovered software vulnerabilities should be disclosed or retained for national security purposes.[[109]](#footnote-110)

The Defense Production Act allows the Department of Commerce to influence foreign-based companies linked to U.S. intellectual property.[[110]](#footnote-111) For instance, in 2021, the U.S. compelled Taiwan-based TSMC to disclose sensitive customer information, including ties to Chinese firms, due to its heavy dependence on U.S. IP, suppliers, and markets.[[111]](#footnote-112)

 Amid growing strategic competition with China, the Export Control Reform Act of 2018 (ECRA) reestablished statutory authority over dual-use controls and expanded executive power to regulate emerging technologies.[[112]](#footnote-113) As Whang notes, ECRA marked a turning point: export controls became tools of economic policy aimed at sustaining U.S. dominance in innovation.[[113]](#footnote-114)

This trend intensified under the Biden administration, which introduced broad export restrictions targeting the semiconductor sector. These covered not just specific technologies, but entire categories of high-performance chips and production equipment.[[114]](#footnote-115) Though justified on national security grounds—primarily the need to limit China’s AI capabilities—they also served economic and industrial policy objectives. However, these measures have also created domestic risks: leading U.S. firms like NVIDIA, AMD, and Intel face substantial revenue losses due to reduced global market access.[[115]](#footnote-116)

In January 2025, during its final days in office, the Biden administration implemented the Framework for AI Diffusion, an Interim Final Rule (IFR) designed to prevent indirect semiconductor transfers to China via third-party countries.[[116]](#footnote-117) The IFR introduced country- and entity-specific licensing requirements, effectively barring Chinese firms from acquiring high-performance AI chips without Department of Commerce approval.[[117]](#footnote-118)

In response, China accelerated domestic chip production and imposed export restrictions on critical minerals such as gallium and germanium—both essential for semiconductor manufacturing.[[118]](#footnote-119) These developments underscore the dual function of export controls: containing risk while serving as instruments of industrial and strategic competition.

Finally, International Humanitarian Law (IHL) imposes independent constraints on the development and transfer of military technologies. Article 36 of the First Additional Protocol to the Geneva Conventions requires states to assess the legality of new weapons and methods of warfare to ensure compliance with international law.[[119]](#footnote-120) These reviews apply regardless of whether technologies are developed domestically or sourced from abroad. Although IHL does not mandate a specific methodology, states employ various review mechanisms to evaluate legal and ethical standards in emerging military technologies.[[120]](#footnote-121)

### Dominant Regulatory Models

Not being the initiators, governments must align with innovative tech companies' interests, whether through persuasion or coercion.[[121]](#footnote-122) Various governments employ different regulatory models to advance military technological progress and encourage collaboration between the private and public sectors. This subchapter will survey the three dominant regulatory models according to Bradford's Digital Empires: The United States market-driven model, the Chinese state-driven model, and the EU's rights-driven model. Each model reflects distinct theories about the relationship between markets and innovation, the role of the state, and the balance between personal and public rights.[[122]](#footnote-123)

Bradford describes the U.S. model as one that prioritizes incentives for innovation.[[123]](#footnote-124) This market-driven approach relies heavily on the ability of tech companies to self-regulate, with minimal government intervention, except through subsidies.[[124]](#footnote-125) The government’s role is generally limited, except in areas concerning national security, including cybersecurity, where the government and the private sector collaborate to address threats and ensure protection.[[125]](#footnote-126)

The Chinese state-driven regulatory model is characterized by the use of technology as a tool to reinforce centralized government authority.[[126]](#footnote-127) This approach has become a defining force in shaping China’s domestic tech industry. Regulatory control is exercised primarily through party oversight rather than legal transparency, reflecting a governance system that prioritizes political stability and strategic objectives over procedural openness.[[127]](#footnote-128)

A core element of this model is the classification of data as a national asset. The Chinese government enforces this principle through an extensive framework of laws, policies, and administrative measures.[[128]](#footnote-129) Companies—both domestic and foreign—are granted access to the Chinese market only if they comply with centralized data governance requirements, including the legal obligation to store data on government-operated servers. Market participation is effectively conditioned on alignment with state-defined strategic interests.[[129]](#footnote-130)

In addition, the Chinese government actively supports domestic technology firms through financial subsidies and protective trade policies.[[130]](#footnote-131) This regulatory model enables the state to set research priorities, coordinate closely with private enterprises, and maintain a high degree of secrecy around technological advancements. While this system facilitates rapid development and strategic coherence, it may also limit openness, restrict international collaboration, and suppress independent innovation within the private sector.[[131]](#footnote-132)

The European rights-driven regulatory model prioritizes the protection of individual and collective rights.[[132]](#footnote-133) It supports active regulatory intervention to safeguard human rights, uphold democratic values, and ensure that technological advancement promotes, rather than undermines, civic freedoms.[[133]](#footnote-134)

These three regulatory models—the U.S. market-driven, Chinese state-driven, and European rights-driven—reflect different frameworks for overseeing innovation and managing public-private collaboration. As later chapters will discuss, the rise of AI has intensified geopolitical competition, shaping how states perceive national security and structure innovation policy.[[134]](#footnote-135)

Huq argues that such geopolitical pressures are likely to influence all three models. Under increasing external threats, governments may reduce protections for individual rights and deepen cooperation with domestic technology firms. Historically, heightened global competition has correlated with a shift away from libertarian governance and toward more centralized, state-led approaches—even in regions with strong commitments to civil liberties.[[135]](#footnote-136)

# Chapter 2: Military Tech-Transfer in the Age of AI

Building on the previous chapter's examination of the historical and regulatory foundations of military tech-transfer, this chapter analyzes how recent advancements in AI are reshaping the dynamics of military tech-transfer. It focuses on two core elements driving this transformation: the unique technological characteristics of AI and the evolving ecosystem in which military AI is developed and deployed.

Together, these elements challenge the traditional boundaries between civilian and military applications. They also underscore the growing interdependence between the public and private sectors in advancing military innovation. This chapter explores each of these drivers and their implications for regulatory adaptation.

## Technological Characteristics of AI

Since 2000, AI has evolved rapidly, moving from experimental research into widespread use across domains such as design, manufacturing, and defense.[[136]](#footnote-137) This growth stems from the convergence of three foundational elements: the availability of big data, advances in ML, and increases in computational power.[[137]](#footnote-138) Though definitions vary, AI can broadly be understood as a set of algorithmic tools that simulate or enhance human cognitive processes by analyzing large datasets.[[138]](#footnote-139)

The global race to AI is shaped by several foundational technological components: access to large-scale datasets, advanced computational infrastructure, sophisticated ML models, and the increasing reliance on cloud-based services that enable scalable development and deployment.[[139]](#footnote-140) These elements collectively determine a nation’s or firm’s ability to innovate in AI and thus have become central to geopolitical and economic strategy.[[140]](#footnote-141) The following subchapter examines these components in greater detail, highlighting their technical function and strategic implications.

### Data Dependency and Computational Demands

AI systems rely heavily on high-quality, large-scale datasets to train algorithms and produce accurate, adaptable results.[[141]](#footnote-142) AI not only depends on data but also serves as a powerful mechanism for extracting knowledge and strategic insights from it.[[142]](#footnote-143)

Managing this data requires substantial computing power, especially for training deep learning models. Advances in cloud computing have dramatically increased AI capabilities, allowing providers—primarily Big Tech companies—to dominate the field.[[143]](#footnote-144) These firms also maintain critical alliances with hardware manufacturers, chipmakers, and data center providers, reinforcing new interdependencies in the AI landscape. Moreover, the energy demands of large-scale AI models make access to affordable and reliable power sources an increasingly strategic concern.[[144]](#footnote-145)

### Machine Learning and the “Black Box” Problem

ML uses statistical algorithms to replicate human cognitive tasks by analyzing large datasets to identify patterns and derive rules.[[145]](#footnote-146) These algorithms learn from prior inputs to perform similar tasks on new data.[[146]](#footnote-147) Deep learning, a subset of ML, uses neural networks that emulate human brain functions to adjust and improve over time.[[147]](#footnote-148)

Unlike traditional technologies, AI is often acquired as software or service modules that are adaptable and easily integrated into other systems.[[148]](#footnote-149) However, a defining feature of many AI systems is their “black box” nature—complex internal processes that are difficult to interpret, even by their developers.[[149]](#footnote-150) This opacity poses challenges for accountability and oversight, especially in high-risk contexts like military operations.[[150]](#footnote-151)

### AI in Military Applications and ISR

The American DoD notes a key distinction between traditional software and AI: while the former performs tasks using fixed instructions, AI systems use algorithms to learn and evolve based on new data inputs. This adaptability makes AI especially powerful for military applications that require rapid decision-making.[[151]](#footnote-152)

AI is currently used across military domains including logistics, cybersecurity, command and control, autonomous systems, and weapons targeting.[[152]](#footnote-153) This research focuses on AI's role in intelligence, surveillance, and reconnaissance (ISR)—a domain increasingly overwhelmed by “data overload.” AI’s ability to filter and analyze vast amounts of data has become essential to enhancing situational awareness and operational efficiency.[[153]](#footnote-154)

AI-powered tools like image recognition, computer vision, and natural language processing are particularly effective in ISR tasks.[[154]](#footnote-155) For example, "Project Maven", a partnership between Google and the DoD, demonstrated AI’s capacity to process drone footage and assist with real-time battlefield analysis.[[155]](#footnote-156)

Unmanned Aerial Vehicles (UAVs), or drones, represent one of the most visible military uses of AI.[[156]](#footnote-157) Originally used for reconnaissance, drones evolved into offensive tools during conflicts such as the post-9/11 wars and, more recently, in Ukraine and Gaza.[[157]](#footnote-158) AI-driven drones are now equipped with real-time pattern recognition and facial recognition capabilities, enhancing military decision-making.[[158]](#footnote-159)

According to the official publication of the Israeli Ministry of Defense, during the current Israel-Gaza war, the Israeli Defense Forces (IDF) deployed AI systems for intelligence analysis and threat detection.[[159]](#footnote-160) Systems like “The Gospel” and “Lavender” cross-reference intelligence data to identify potential targets. These platforms use AI to classify individuals based on behavioral similarity to known operatives, significantly streamlining military operations.[[160]](#footnote-161)

Other AI applications include threat detection systems like "Alchemist" and missile defense platforms like "Iron Dome", which use AI for real-time threat analysis, interceptor prioritization, and launch optimization. These systems have proven effective in neutralizing missile and drone attacks, including multi-front threats from Gaza, Lebanon, Syria, Yemen, and Iran.[[161]](#footnote-162)

By automating processes previously handled by human analysts, AI enhances both the speed and accuracy of decision-making in ISR contexts. As the next subchapter will show, these capabilities are deeply intertwined with the broader military AI ecosystem and the collaborative dynamics shaping tech-transfer in the AI age.

## Military AI Ecosystem

The development of military AI involves an intricate network of stakeholders that can be broadly categorized into public and private sectors, each with distinct approaches and priorities. The private sector includes a diverse array of entities, from small startups to Big Tech. In contrast, public sector entities are shaped by geopolitical factors, regulatory priorities, and security interests.

This subchapter begins by examining the public sector within its geopolitical context, often referred to as the AI arms race. It then explores the critical importance of collaboration between the public and private sectors in the field of AI, emphasizing the key reasons such partnerships are vital.

### The AI Arms Race

The global competition surrounding AI is often called a "Tech Race" or "AI arms race.".[[162]](#footnote-163) Those terms are used metaphorically to refer to the broader competition among the world's major powers for technological dominance in AI.[[163]](#footnote-164) To achieve this, government entities are crucial in funding and regulating technological development and are eager to pursue AI capabilities for national security and power enhancement.[[164]](#footnote-165)

The United States and China dominate this race.[[165]](#footnote-166) China has made strategic investments across sectors including surveillance, governance, and defense, positioning AI as a cornerstone of national policy through initiatives like the *Next Generation AI Development Plan*. A key advantage lies in its tightly integrated system that merges state, military, academic, and corporate efforts.[[166]](#footnote-167) China’s limited emphasis on privacy also facilitates large-scale data collection, a critical input for AI development.[[167]](#footnote-168)

The U.S. maintains leadership through its innovative commercial ecosystem, leading research institutions, and democratic governance, which facilitates international collaboration.[[168]](#footnote-169) Successive U.S. administrations have prioritized AI: from the Obama administration’s 2016 report on AI to the 2019 *American AI Initiative*, which promoted government–industry–academia partnerships for AI advancement.[[169]](#footnote-170) The establishment of the Joint AI Center (JAIC) in 2018 further institutionalized military AI development.[[170]](#footnote-171)

Although the U.S. remains a leader, China’s aggressive pursuit of military AI has intensified global competition.[[171]](#footnote-172) Meanwhile, the European Union plays a major role in shaping global AI regulation. Its 2018 coordinated AI plan and later adoption of the AI Act reflect a cautious and ethics-oriented approach, which, while normatively influential, has proven reactive and slower than American and Chinese efforts.[[172]](#footnote-173)

This race has reshaped regulatory thinking, particularly around military tech-transfer. Economic competitiveness now rivals national security as a policy driver, giving rise to new regulatory priorities that blend geoeconomic and security concerns.[[173]](#footnote-174)

A distinctive feature of this competition is the central role of private tech companies. Controlling vital data, infrastructure, and communications networks, these firms now act as de facto geopolitical players. Their involvement is transforming how states access, develop, and deploy military AI.[[174]](#footnote-175) The next subchapter explores the evolving nature of this public-private collaboration.

### The Significance of Public-Private Collaboration

In the era of AI, the private sector plays an increasingly critical role in military innovation. Many key technologies now originate in civilian firms rather than defense labs. As a result, national security institutions have become increasingly dependent on private companies to access cutting-edge AI capabilities.[[175]](#footnote-176)

Big Tech firms, in particular, drive innovation more rapidly than government agencies, unburdened by bureaucratic inertia.[[176]](#footnote-177) Companies like Alphabet (Google), Microsoft (via OpenAI), and SpaceX are global leaders in AI, space, and data technologies. In parallel, companies like Apple and Amazon have expanded into sectors such as healthcare, showcasing the adaptability and scale of private innovation.[[177]](#footnote-178)

Governments now actively partner with the private sector to harness commercial advancements for defense.[[178]](#footnote-179) This cooperation takes several forms: data sharing, cloud infrastructure provisioning, investment in dual-use startups, and adaptation of civilian technologies for military applications.

#### Control over Data

Data is the foundational resource for AI development. However, military organizations face structural constraints in acquiring and using data, such as classification rules and limited access to cloud platforms. This hinders their ability to train adaptable algorithms.[[179]](#footnote-180) In contrast, private firms accumulate vast datasets from user interactions, devices, and services.[[180]](#footnote-181)

Big Tech companies build their business models on platforms that connect users on one side of the market with users on the other side for transactions or interactions.[[181]](#footnote-182) For example, the Chinese app WeChat, also called "app of everything", allows users to share text, voice, and video messages, play video games, pay for goods and services, engage in video conferencing, and use other services, including disease monitoring. WeChat is a subsidiary of the Chinese Big Tech company Tencent.[[182]](#footnote-183) Platforms tend to exhibit network effects—adding a new user increases the value of a platform to existing users and attracts new users. Once a platform sets the network effect flywheel in motion, its position can be hard to dislodge.[[183]](#footnote-184)

 Such data is highly valuable: it improves product development, supports behavioral targeting, and trains more effective AI models[[184]](#footnote-185) Scholars like Rolf and Schindler argue that both the U.S. and China leverage their domestic tech sectors to project global influence.[[185]](#footnote-186) Similarly, Kokas, in *Trafficking Data*, contends that U.S. tech firms act as unofficial arms of national strategy, complicating regulatory control.[[186]](#footnote-187)

#### Cloud and Infrastructure Providers

Big Tech companies play a central role in the cloud computing market, offering comprehensive services that support the entire lifecycle of AI development. These services include data storage, data processing, algorithm training, and deployment platforms. Organizations that lack the internal resources to build or maintain such capabilities often turn to commercial providers to access computing power, pre-configured environments, and specialized development tools.[[187]](#footnote-188)

Reliance on commercial cloud infrastructure has significantly accelerated AI adoption in both civilian and military contexts. Defense agencies now depend on private providers—particularly Amazon, Microsoft, and Google—to enhance operational and analytical capabilities.[[188]](#footnote-189) For instance, AWS and Microsoft offer secure platforms tailored to intelligence and national security needs.[[189]](#footnote-190) The 2020 Commercial Cloud Enterprise (C2E) contract, awarded by the CIA to five major tech firms, institutionalized this reliance by modernizing cloud services across U.S. intelligence agencies.[[190]](#footnote-191)

Cloud providers not only deliver computing capacity but also benefit from the data generated by their clients. Unlike traditional technologies, cloud-based AI systems continuously improve through user engagement. As algorithms process new inputs, they are refined and updated in real time, creating self-reinforcing cycles of improvement.[[191]](#footnote-192) Consequently, each user interaction contributes to the enhancement of the underlying technology. This feedback loop solidifies the technological leadership of cloud providers and strengthens their competitive advantage.[[192]](#footnote-193)

The relationship between cloud providers and their clients is thus more than transactional. It fosters a form of strategic dependency, whereby users rely not only on infrastructure but also on the continued development and evolution of AI technologies controlled by private firms.[[193]](#footnote-194)

#### Investments in Innovation

Private-sector investment also drives AI development.[[194]](#footnote-195) Leading firms such as DeepMind, OpenAI, Anthropic, and Inflection started as independent ventures but now operate in close partnership with or under the influence of Big Tech funders.[[195]](#footnote-196) These companies support innovation through venture capital, acquisitions, and startup accelerator programs.[[196]](#footnote-197)

The dual-use nature of AI technologies, applicable in both civilian and military contexts, creates a lucrative market that motivates sustained investment.[[197]](#footnote-198) Big Tech has shown a growing interest in investing in AI start-ups. A notable instance of this is the launch of the ‘AWS European Defense Accelerator’ by Amazon Web Services (AWS) in early 2023, in partnership with a technology firm supported by the UK government. This initiative is designed to train and support a select group of start-ups in leveraging AWS cloud technologies to develop defense-related technologies and capabilities that enhance national security organizations throughout Europe.[[198]](#footnote-199)

Big Tech companies have launched AI startup programs to attract and support emerging AI businesses. These programs provide valuable resources, such as cloud credits, specialized training, technical support, webinars, and access to experts, often at no initial cost. This approach encourages startups to join their ecosystems, positioning Big Tech as essential partners in their growth. By lowering financial barriers and offering development tools, these companies foster a network of innovators that strengthens their infrastructure and services for future AI applications.[[199]](#footnote-200)

#### Adapting Commercial Technologies for Military Use

The ongoing Russo-Ukrainian and Hamas-Israel wars underscore the unprecedented speed with which commercial technologies are being adapted for military purposes. These conflicts reveal how off-the-shelf platforms and services—originally developed for civilian markets—can be rapidly integrated into national defense operations.

In Ukraine, cooperation between the government and private tech firms has led to innovative uses of AI in warfare.[[200]](#footnote-201) Technologies originally not intended for military use have been adapted for combat.[[201]](#footnote-202) For instance, Ukrainian drones equipped with AI and connected to SpaceX's Starlink satellite network can autonomously identify targets, chart flight paths, and gather real-time intelligence.[[202]](#footnote-203) Starlink, which provides high-speed broadband globally, became crucial for Ukraine after Elon Musk made it available during the early war days, ensuring secure communication in conflict areas.[[203]](#footnote-204)

AI has also been used by Ukraine in FRT.[[204]](#footnote-205) Clearview AI, a U.S.-based company, offered its system to Ukraine’s defense ministry to help identify Russian personnel, counter disinformation, and account for casualties.[[205]](#footnote-206) The system, trained on billions of publicly sourced images, demonstrated the utility of FRT in real-time military contexts.[[206]](#footnote-207) Although FRT has been deployed in previous conflicts, its open use and field deployment at the outset of the Ukraine war marked a turning point in its military adoption.[[207]](#footnote-208)

Palantir Technologies, headquartered in the UK, has contributed extensively to Ukraine’s defense infrastructure. Originally designed for fraud detection, Palantir’s tools have been adapted for military use, integrating satellite imagery, drone footage, and open-source intelligence into actionable battlefield insights.[[208]](#footnote-209) Reports suggest Palantir provided its services free of charge, further extending its applications to war crimes documentation, refugee resettlement, and anti-corruption efforts.[[209]](#footnote-210)

Big Tech companies, including Microsoft and Amazon, have provided cybersecurity support and helped migrate sensitive Ukrainian government data to the cloud. These in-kind contributions, valued in the hundreds of millions of dollars, highlight the growing role of Big Tech in national defense efforts.[[210]](#footnote-211)

The war has turned Ukraine into a live testing environment for emerging technologies. The realities of combat offer companies the chance to refine systems that would be difficult to evaluate domestically. This symbiotic relationship benefits both sides: states gain advanced capabilities, and companies collect operational feedback while boosting their reputations. [[211]](#footnote-212)

A similar pattern has emerged in the Hamas-Israel war. The IDF and intelligence agencies have extensively utilized AI systems for tasks such as identifying victims of the October 7th massacre by analyzing body tissues and remains.[[212]](#footnote-213) AI has also been deployed in target analysis and command-level intelligence operations, using geospatial and open-source intelligence integrated with historical datasets to provide actionable insights.[[213]](#footnote-214)

A distinctive technological feature of the war in Gaza is the deployment of solutions developed by small startup companies, many of which had not previously been utilized in military operations.[[214]](#footnote-215) Israeli companies like Xtend and Robotican,[[215]](#footnote-216) specializing in drones and robotics, have played pivotal roles in navigating and patrolling confined spaces, including buildings, shafts, and tunnels.[[216]](#footnote-217) These technologies have not only been instrumental in saving lives but have also significantly bolstered the war effort by enabling proactive measures to counter threats before direct confrontations arise.[[217]](#footnote-218)

In response to the conflict, these and other small tech companies have received substantial government support, facilitated by emergency measures that include flexible financial and regulatory frameworks. This backing has allowed these startups to adapt and scale their innovations to meet the demands of modern warfare.[[218]](#footnote-219)

Access to conflict areas provides commercial companies with a unique test-bed for testing, evaluating, and adapting new technologies. Accordingly, the battlefield becomes a peculiar laboratory that allows for experimentation, testing, and refinement of military technologies that, in some cases, may prove transferable and profitable in the civilian domain as well.[[219]](#footnote-220) At the same time, as Big Tech becomes an essential partner in conducting an increasing number of military activities, the government tends to build stable alliances with these companies.[[220]](#footnote-221)

In her article, Agne Limante discussed several incentives for companies contributing to the Russo-Ukrainian war. She highlighted that, from the companies' perspective, applying AI technologies to the Ukrainian war effort offers visibility and serves as an advertisement for firms involved in this field.[[221]](#footnote-222) Wartime deployment provides an opportunity to demonstrate the effectiveness of their technologies in real-world, high-pressure scenarios. As a result, companies whose products are utilized in this conflict, on both sides, are likely to transition into defense contractors, further marketing their technologies for military applications.[[222]](#footnote-223)

Such motivations likely influenced NATO’s decision to contract Palantir in March 2025 to implement its NATO Mission Management System. This project will integrate AI tools to improve intelligence gathering, situational awareness, and command decision-making across NATO’s operational framework.[[223]](#footnote-224)

Further underscoring this reputational effect, Lilly’s research cites Microsoft’s role in Ukraine as a model of wartime innovation.[[224]](#footnote-225) The company’s AI-based Defender for Endpoint system reportedly blocked Russian malware without prior signatures and allowed rapid deployment of patches across its global cloud infrastructure. These achievements enhanced Microsoft’s stature as a key cybersecurity actor.[[225]](#footnote-226)

These developments highlight a broader shift in how states acquire advanced defense technologies. Rather than relying solely on traditional procurement channels, governments are increasingly integrating commercial solutions that offer lower costs, rapid deployment, and modular scalability. Starlink, for instance, proved faster to implement and more cost-effective than conventional military satellite systems.[[226]](#footnote-227)

## Interim Conclusions

Chapters 1 and 2 traced the evolution of military Tech-Transfer from its traditional foundations—defined by relatively linear, one-directional flows between military and civilian sectors—to a far more complex, interdependent dynamic shaped by AI. Historically, regulatory frameworks were designed around tangible technologies and assumed clear boundaries between applications. However, the emergence of AI has fundamentally disrupted this paradigm.

AI’s reliance on large-scale, cross-sectoral datasets and its capacity for continuous learning has eroded the distinction between civilian and military domains. These changes are further compounded by structural developments: the rise of globally integrated cloud infrastructure, the central role of private-sector actors—especially Big Tech—and the geopolitical race for AI supremacy. Together, these trends reveal a growing public-private interdependence that challenges the core assumptions of existing military tech-transfer regulation.

These developments prompt critical regulatory questions that will be explored in Chapter 3. Through a case study of FRT, followed by a broader legal analysis, the chapter examines where and how current frameworks fall short—and considers preliminary pathways for reform.

# Chapter 3: Tech-Transfer Regulatory Challenges in the Age of AI

This chapter builds on the preceding analysis of how AI has reshaped military tech-transfer and the ecosystems that support it. It focuses on identifying specific regulatory gaps and legal complexities that arise from this transformation. In particular, the chapter examines how AI’s technological features, the evolving military innovation environment, and growing public-private interdependence challenge the effectiveness of existing regulatory frameworks.

The chapter is divided into two main subchapters. The first presents a case study on FRT, a prominent example of AI-based dual-use innovation. It illustrates how overlapping civilian and military applications complicate regulation. The second subchapter expands on this analysis, identifying broader regulatory shortcomings and examining the legal, structural, and strategic challenges that must be addressed to adapt military tech-transfer regulation for the AI era.

## Facial Recognition Technology: Case Study

FRT involves capturing an individual's image and identifying them by analyzing and mapping their facial features, comparing these to known likenesses.[[227]](#footnote-228) It has a wide range of applications, from enhancing consumer convenience, such as contactless payments and personalized advertising, to law enforcement, immigration control, and military operations.[[228]](#footnote-229) Despite its benefits, FRT raises significant concerns about privacy, bias, and surveillance.[[229]](#footnote-230)

Big Tech companies play a central role in FRT development. They control essential infrastructure such as cloud computing and AI algorithms for image recognition, behavior prediction, and targeting.[[230]](#footnote-231) These companies are key actors in military innovation, enabling the adaptation of civilian technologies for defense purposes and supporting R&D through collaborations with startups.[[231]](#footnote-232)

FRT exemplifies the challenges posed by dual-use AI. It demonstrates how one technological base can serve multiple sectors with overlapping datasets and objectives. As discussed below, its deployment across civilian, law enforcement, immigration, and military contexts highlights the legal and regulatory gaps that emerge when a single technology evolves into a shared platform with far-reaching implications.

### Law Enforcement applications

Facial recognition has long been used in law enforcement, but its scope has expanded significantly in the twenty-first century with the integration of AI.[[232]](#footnote-233) These advancements have enabled large-scale, real-time image matching, increasing both speed and operational efficiency. However, they have also introduced new concerns, particularly regarding accuracy and systemic bias.[[233]](#footnote-234)

Bias in AI often stems from unrepresentative training data or historical datasets reflecting existing social disparities.[[234]](#footnote-235) In FRT, the over-representation of minority groups in police databases exacerbates these biases, increasing the likelihood of these individuals being disproportionately identified.[[235]](#footnote-236) This feedback loop directs enforcement toward already-marginalized communities.[[236]](#footnote-237) Similar risks apply in military contexts, where systems trained on selective datasets may inadvertently replicate these biases.

Legal challenges surrounding FRT intensified after the 2020 protests following George Floyd’s death.[[237]](#footnote-238) In addition to privacy concerns, FRT raises broader civil liberties issues, including potential infringements on free expression and assembly. The ability to identify individuals at public demonstrations threatens to deter lawful protest, highlighting the need for stronger safeguards.[[238]](#footnote-239)

### Immigration Enforcement Applications

FRT is increasingly utilized in immigration enforcement, particularly at the U.S. border, where advanced surveillance systems have become standard.[[239]](#footnote-240) While intended to improve security and streamline processing, these systems raise concerns about bias, inaccuracies, and unchecked discretion in an already sensitive policy area.[[240]](#footnote-241)

In the Israel-Palestine context, FRT has reportedly been deployed at border checkpoints using software developed by the Israeli company AnyVision, now rebranded as Oosto.[[241]](#footnote-242) Media reports suggest that the Israeli military constructed a comprehensive database by merging CCTV footage, social media content, and photos taken by patrolling soldiers to monitor Palestinians.[[242]](#footnote-243) Although AnyVision denies involvement, reports indicate that the program utilizes technologies similar to those found in its commercial products, which integrate facial and body recognition with ML to detect and identify suspicious behavior.[[243]](#footnote-244)

### Military Applications

Military use of FRT reflects its growing role in modern warfare. While there are strict restrictions on training FRT in civilian contexts,[[244]](#footnote-245) the military domain is considered an exception.[[245]](#footnote-246) This implies that companies developing FRT models are allowed, or at least not restricted, to train and utilize their models in armed conflicts, as seen in the cases of the Russo-Ukrainian and the Israel-Hamas wars.[[246]](#footnote-247)

In Ukraine, Clearview AI began providing its FRT technology to the government shortly after the Russian invasion in February 2022.[[247]](#footnote-248) By March, the Ministry of Defense had integrated the system into military operations, reportedly using it to identify deceased Russian soldiers and counter disinformation.[[248]](#footnote-249) This practice also expanded Clearview’s database with images collected from the battlefield and war-zone screenings, raising ethical and privacy concerns.[[249]](#footnote-250)

In Israel, FRT was used in both humanitarian and combat roles during the Hamas-Israel war. Amazon’s Rekognition assisted in identifying hostages and captors through social media footage.[[250]](#footnote-251) Hospitals used Corsight AI’s technology to match facially injured patients with family-submitted photos.[[251]](#footnote-252) According to The New York Times, the IDF used FRT—potentially developed by Corsight and supported by Google Photos—to identify Hamas operatives, including from low-quality drone imagery.[[252]](#footnote-253)

Corsight’s Facial Intelligence platform, originally designed for airport security, detects watchlisted individuals, monitors unusual behavior, and integrates seamlessly with existing camera infrastructure. These capabilities have been adapted to enhance operational efficiency and situational awareness in high-risk environments.[[253]](#footnote-254)

### Civilian Applications

Although commonly associated with law enforcement and military operations, FRT is increasingly integrated into civilian sectors such as retail, finance, transportation, and workplace management. In retail, FRT is used to deter theft, offer personalized services, and streamline checkout processes.[[254]](#footnote-255) Banks apply the technology to enhance security and enable seamless customer authentication.[[255]](#footnote-256)

Airports and transit hubs have adopted FRT to manage passenger flows efficiently and bolster security screening.[[256]](#footnote-257) Similarly, workplaces use facial recognition for employee identification, access control, and attendance monitoring.[[257]](#footnote-258) As FRT continues to expand across diverse domains, it is shaping everyday interactions and embedding itself into routine social and economic functions.

### Legal Implications

FRT is not a novel concept; historically, its uses were clearly delineated, each with its own dataset and context. However, AI integration has transformed this paradigm, blurring boundaries between applications and creating shared data ecosystems. As noted in previous chapters, AI’s software-based flexibility enables a single technological infrastructure to support diverse functions across public and private sectors.

For example, Clearview AI, initially developed for law enforcement, was later adapted for military use in Ukraine.[[258]](#footnote-259) Similarly, Corsight AI has applied its FRT across banking, healthcare, law enforcement, and defense sectors.[[259]](#footnote-260) These developments reflect a shift from linear tech-transfer models to circular, mutually reinforcing flows of innovation, where civilian and military domains increasingly overlap.

This evolution raises legal questions about access to and control of military data by commercial firms, especially given the "black box" nature of AI models.[[260]](#footnote-261) Elkin-Koren highlights that AI systems often operate across institutional lines—military, government, and corporate—creating a shared logic of decision-making shaped by both public interest and commercial incentives. As such, decisions in one domain can carry normative consequences in others.[[261]](#footnote-262)

Because AI relies on historical data to predict future behavior, an individual’s classification in one context can influence outcomes in another, even across sectors. When private firms operate globally, national-level regulatory decisions—such as law enforcement database use—can unintentionally shape standards across borders, challenging state sovereignty and regulatory consistency.[[262]](#footnote-263)

## Regulatory Gaps

The preceding subchapter on FRT revealed several regulatory gaps stemming from the convergence of applications and the reliance on vast, overlapping datasets. This chapter builds on those insights by examining the broader legal and regulatory challenges unique to military tech-transfer in the AI era. It considers how these challenges are compounded by both the technical characteristics of AI and the surrounding innovation ecosystem. Additionally, it addresses the conflicting interests among stakeholders—public and private—that shape and complicate the regulatory landscape.

### Access to Data, Sharing, and IP rights

A core challenge in developing military AI lies in securing high-quality datasets for model training. Private firms typically access such data through government partnerships or by scraping open-source intelligence, including synthetic data generation.[[263]](#footnote-264) Because AI performance depends on data quantity, diversity, and quality, data acquisition raises complex regulatory issues.[[264]](#footnote-265) Key questions include whether access should be controlled by technological safeguards, legal mechanisms, or a combination of both—and whether restricting data might hinder AI performance.

Current legal literature focuses primarily on data sharing between private firms and law enforcement, especially regarding privacy.[[265]](#footnote-266) Yet this overlooks the AI-specific challenge of mutual dependence: civilian and military systems increasingly rely on one another’s data. This is especially evident in wartime, where commercial firms may seek to use conflict-generated data to refine products, while states prioritize secrecy and national security.

Governments themselves face a dual imperative. While restricting access to combat data is critical for security, doing so may also inhibit AI system improvement. This creates internal tensions over whether to protect or share sensitive operational datasets.[[266]](#footnote-267)

Ownership further complicates data governance. U.S. defense procurement law allocates “data rights” via copyright licenses and trade secrets.[[267]](#footnote-268) However, modern AI systems are not static; they evolve with continued data input. This makes it difficult to separate civilian from military data, and nearly impossible to trace how specific datasets shape model behavior.

China’s Military-Civil Fusion (MCF) strategy, by contrast, mandates corporate data-sharing with the military, enabling the state to exploit both domestic and foreign tech partnerships.[[268]](#footnote-269) This underscores a regulatory gap in Western frameworks, where commercial and national interests often conflict.

Ultimately, traditional IP regimes—designed for fixed products—are ill-equipped to manage AI’s continuous learning. Retrainable systems defy one-time ownership models and necessitate clearer rules around access, control, and accountability across public-private boundaries.[[269]](#footnote-270)

### Governance and Oversight

The AI development lifecycle now moves bidirectionally—between the private sector and the state—creating a shared responsibility for the quality and implications of the technologies produced. As discussed, both commercial firms and governments benefit from deploying civilian AI-based surveillance platforms in military contexts. However, when data collected in conflict zones is later reused in civilian applications, performance may degrade or yield unintended consequences. Although regulations often restrict the training of algorithms on sensitive civilian data, oversight remains limited in national security and intelligence contexts, particularly for battlefield applications.

This raises critical questions: Should the training of AI systems on combat-related data be subject to limits? Who is responsible for potential biases or unintended consequences when data is recycled across military and civilian systems? AI systems, especially those with limited explainability, present inherent risks that challenge traditional concepts of accountability.[[270]](#footnote-271) Yet existing frameworks rarely address the risk of algorithmic bias in military AI, even though such biases may carry over into commercial settings.

The increasing reliance on private-sector developers introduces further complications. Many companies assert trade secret protections to shield their algorithms, training data, and input parameters from public scrutiny.[[271]](#footnote-272) These legal protections can form a “black box,” limiting transparency and potentially conflicting with due process rights.[[272]](#footnote-273) A recent Federal Circuit case, though unrelated to AI, affirmed that trade secret protections must yield when they undermine procedural fairness—a principle increasingly relevant in the AI domain.[[273]](#footnote-274)

Export control regimes, such as the WA, also struggle to adapt. They lack clear criteria to distinguish between civilian and military AI applications, hindering enforcement.[[274]](#footnote-275) Furthermore, these controls were designed for tangible goods and software, not cloud-based services. AI delivered through Software-as-a-Service (SaaS) platforms often transcends national boundaries, making it difficult to regulate effectively under traditional frameworks.[[275]](#footnote-276)

Some scholars, like Fideler, propose shifting from technology-based to entity-based export controls. This approach would target specific actors—such as human rights violators or adversarial governments—rather than attempting to classify and restrict rapidly evolving technologies. It offers greater flexibility in addressing contemporary security risks.[[276]](#footnote-277)

Other researchers highlight how stringent export controls may inadvertently hinder innovation. Berkowitz argues that regulating digitally transferrable technologies is increasingly ineffective.[[277]](#footnote-278) Stowsky adds that secrecy surrounding dual-use technologies is difficult to maintain and instead advocates for building strategic partnerships between governments and industry to promote both innovation and security.[[278]](#footnote-279)

Finally, oversight is also hampered by the diversity of actors in the military AI ecosystem. Many non-state entities, including small firms and startups, lack the capacity to build robust compliance mechanisms. This lack of institutional awareness increases the risk of unintentional proliferation and regulatory non-compliance, underscoring the need for a more comprehensive oversight infrastructure.[[279]](#footnote-280)

### Infrastructures

Commercial companies, particularly Big Tech firms, have become indispensable partners to the military sector due to their control over critical digital infrastructure and AI technologies.[[280]](#footnote-281) These companies not only provide the data and tools necessary for modern military operations but also dominate the broader innovation ecosystems from which security-related advancements emerge.[[281]](#footnote-282)

Another emerging regulatory concern is the growing dependence of AI systems on vast energy resources and robust digital infrastructure, particularly cloud data centers. These facilities are essential for powering AI development and deployment but are also increasingly vulnerable to cyberattacks and other security threats. The risks are compounded by the fact that most of this infrastructure is privately owned and operated, leaving national defense systems dependent on commercial entities for foundational security elements.[[282]](#footnote-283)

As AI innovation becomes increasingly inseparable from its supporting infrastructure, new legal and regulatory mechanisms are needed to ensure that these critical assets are adequately protected, transparently governed, and resilient under conditions of national emergency or conflict.

## Conclusion

This chapter has explored various challenges associated with regulating military AI tech-transfer. These challenges include issues related to data access and sharing, IP rights, governance, oversight, and critical infrastructure. Some of these problems may be resolved by updating current regulatory tools, while others require more adaptive and forward-thinking regulatory strategies.

Although the core objectives of military tech-transfer regulation—promoting innovation and protecting national security—are likely to remain constant, they must now be pursued in a more complex and rapidly evolving technological environment. The unique features of AI, along with its innovation ecosystem and the blurring of civilian and military boundaries, demand a fundamental shift in regulatory approach.

Enforcement mechanisms, in particular, must be recalibrated to address AI’s reliance on large, cross-sectoral datasets and continuous learning. Regulatory frameworks must also account for growing public-private interdependencies and the broader geopolitical competition driving AI development.

Effective governance today requires more than risk containment; it calls for a strategic, systems-level understanding of how innovation, regulation, and international competition intersect. This proposal contributes to that effort by identifying key legal questions and outlining areas where existing frameworks may need to evolve.

# Research Question

This research proposal addresses the following central question: **To what extent, and in what ways, should existing regulatory frameworks governing military tech-transfer be adapted to meet the unique challenges posed by the AI era?**

While this proposal has already outlined the objectives and mechanisms of existing military tech-transfer regimes, the proposed research will refine and deepen that analysis. It will also undertake a comparative assessment of both domestic and international regulatory approaches, including models discussed in *Digital Empires*. The study will examine whether traditional distinctions between regulatory regimes remain relevant in the AI context, or whether those boundaries are increasingly blurred by geopolitical and geoeconomic shifts. Particular attention will be given to how these developments may shape the future regulation of defense innovation.

The research will further examine the roles of key stakeholders—particularly startups and Big Tech—and the divergent incentives that shape their involvement in military innovation. A detailed analysis of these actors’ motivations will inform strategies for fostering effective public-private cooperation, a recurring theme throughout this proposal.

Building on this foundation, the study will broaden its analysis to identify and map the major regulatory challenges and gaps that have emerged in the AI era. These will be categorized into key areas in need of legal and policy adjustment. Ultimately, the research will propose legal and regulatory reforms tailored to the evolving technological and strategic landscape. These recommendations will reflect the interests of multiple stakeholders, the incentives driving innovation and collaboration, and the broader geopolitical and structural conditions shaping military tech-transfer.

While much of the current literature on tech-transfer lies outside the legal domain, this research offers a novel contribution by framing these emerging developments within a legal and regulatory context. The relative scarcity of legal scholarship in this area likely reflects the recent and rapid rise of AI-related military applications. However, as the boundary between military and civilian domains becomes increasingly porous, scholars have called for greater legal engagement with these transformations.

Unlike much existing commentary, which tends to focus on the risks of military AI and the need for restraint, this research adopts a more constructive approach. It recognizes both the inevitability and the potential value of military innovation, and aims to support responsible, forward-looking regulation that enables—rather than inhibits—public-private collaboration.

In sum, this proposed research seeks to develop concrete legal recommendations to improve the governance of military tech-transfer in an era of rapid, AI-driven change. As civilian and military sectors become increasingly interdependent and defense innovation grows more dynamic, the need for adaptable and responsive regulatory frameworks is urgent.

1. See detailed discussion of Military Tech-Transfer Dynamics in Chapter 1 of the research proposal. [↑](#footnote-ref-2)
2. See the discussion of the transformation and the reasons that led to it in chapter 2, Military Tech Transfer in the Age of AI. [↑](#footnote-ref-3)
3. Id. [↑](#footnote-ref-4)
4. See detailed discussion of technological characteristics of AI systems in Chapter 2 of the research proposal. [↑](#footnote-ref-5)
5. Id. [↑](#footnote-ref-6)
6. "Big Tech" usually refers to the world's most valuable public companies: the major US-based platforms Microsoft, Amazon, Apple, Alphabet (Google), and Facebook (Meta), and the Chinese Alibaba, ByteDance and Tencent. For more information, see, for instance, Wil van der Aalst, Oliver Hinz & Christof Weinhardt, *Big Digital Platforms*, 61 Bus. & Info. Sys. Eng’g 645 (2019); Andrea Coveri, Claudio Cozza & Dario Guarascio, *Blurring Boundaries: An Analysis of the Digital Platforms–Military Nexus*, Rev. Pol. Econ. (Sept. 3, 2024), <https://doi.org/10.1080/09538259.2024.2395832>; Andrea Coveri, Claudio Cozza & Dario Guarascio, *Big Tech and the US Digital-Military-Industrial Complex*, 60 INTERECONOMICS 81 (2025), https://doi.org/10.2478/ie-2025-0017. [↑](#footnote-ref-7)
7. See detailed discussion on Stakeholders and Geopolitical Influences in Chapter 2 of the research proposal. [↑](#footnote-ref-8)
8. Id. [↑](#footnote-ref-9)
9. See discussion of existing regulation in Chapter 1: Military Tech-Transfer Regulatory Framework. [↑](#footnote-ref-10)
10. See the discussion in Chapter 1 regarding the regulatory framework. [↑](#footnote-ref-11)
11. See Chapter 3 of the research proposal for a discussion on the regulatory gaps in the AI era. This chapter features a section that presents test cases for different FRT, emphasizing some of the expected regulatory challenges. Additionally, it covers broader issues related to these regulatory gaps. [↑](#footnote-ref-12)
12. Although often used interchangeably, *spillover* and *tech-transfer* can denote distinct phenomena. *Spillover* refers to the unintentional diffusion of knowledge or technology across sectors or actors, typically occurring informally. In contrast, *tech-transfer* describes the intentional, structured transmission of knowledge or innovation between organizations, usually for further development or commercialization. See for example: John A. Alic, The Dual Use of Technology: Concepts and Policies, 16 **Tech. in Soc’y** 155 (1994); Carlos Martí Sempere, What Is Known About Defence Research and Development Spill-Overs?, 29 Def. & Peace Econ. 225, 226 (2016). This research adopts *"tech-transfer*" to emphasize deliberate, institutionalized exchanges, as opposed to incidental spillovers. [↑](#footnote-ref-13)
13. Raymond Wang, *Guns and Butter: Measuring Spillover and Implications for Technological Competition* 1 (unpublished draft, 2024); Jordi Molas-Gallart, *Which Way to Go? Defence Technology and the Diversity of ‘Dual-Use’ Technology Transfer*, 26 Res. Pol’y 367, 372 (1997). [↑](#footnote-ref-14)
14. John A. Alic Et Al., Beyond Spinoff: Military And Commercial Technologies In A Changing World 4 (Harv. Bus. Sch. Press 1992). [↑](#footnote-ref-15)
15. Id. [↑](#footnote-ref-16)
16. Jay Stowsky, *The Dual-Use Dilemma*, 13 Issues Sci. & Tech. 56, 58 (1996). [↑](#footnote-ref-17)
17. Molas-Gallart, *supra note* 13, at 367–385. [↑](#footnote-ref-18)
18. Yoram Evron, *The Fourth Industrial Revolution and Military-Civil Fusion: A New Paradigm for Military Innovation?*, in The Fourth Industrial Revolution and Military-Civil Fusion 25-26 (Richard Bitzinger ed., 2023); Fred V. Carstensen, *Review of From the American System to Mass Production, 1800–1932: The Development of Manufacturing Technology in the United States by David A. Hounshell*, 59 Bus. Hist. Rev. 299 (1985). [↑](#footnote-ref-19)
19. Alic , supra note 14, at 4. [↑](#footnote-ref-20)
20. Id. [↑](#footnote-ref-21)
21. Id. [↑](#footnote-ref-22)
22. For a broader discussion, *see* Evron, *supra note* 18, at 38; Alic, supra note 14, at part 1; Thomas Heinrich, *Cold War Armory: Military Contracting in Silicon Valley*, 3 Enterprise & Soc’y 247, 247–49 (2002); David C. Mowery & Richard N. Langlois, *Spinning Off and Spinning On(?): The Federal Government's Role in the Development of the U.S. Computer Software Industry*, in Research Policy 947, 947–48 (David C. Mowery ed., 1996). [↑](#footnote-ref-23)
23. Alic, supra note 14, at 55. [↑](#footnote-ref-24)
24. David C. Mowery & Timothy Simcoe, *Is the Internet a U.S. Invention?—An Economic and Technological History of Computer Networking*, 31 Res. Pol’y 1369, 1370–72 (2002); Jay Stowsky, *Secrets to Shield or Share? New Dilemmas for Military R&D Policy in the Digital Age*, 33 Res. Pol’y 257, 265–68 (2004). [↑](#footnote-ref-25)
25. Richard H. White et al., A Survey of Dual-Use Issues 3–4 (1996). [↑](#footnote-ref-26)
26. Sameer Kumar & Kevin B. Moore, *The Evolution of Global Positioning System (GPS) Technology,* 11 J. Sci. Educ. & Technol. 59 (2002). [↑](#footnote-ref-27)
27. Omid Maghazei, Michael A. Lewis & Torbjørn H. Netland, *Emerging Technologies and the Use Case: A Multi‐year Study of Drone Adoption*, 68 J. Operations Mgmt. 560, 564 (2022); Christian Janke & Maarten Uijt de Haag, *Implementation of European Drone Regulations—Status Quo and Assessment*, 106 J. Intell. Robot. Syst. 32, 32–33 (2022); Marcus Schulzke, *Drone Proliferation and the Challenge of Regulating Dual-Use Technologies*, 21 Int’l Stud. Rev. 497, 500 (2019). [↑](#footnote-ref-28)
28. Evron, *supra note* 18, at 24-25; Alic, supra note 14, at 37. [↑](#footnote-ref-29)
29. Manuel Acosta et al., *Civil–Military Patents and Technological Knowledge Flows Into the Leading Defense Firms,* 46 Armed Forces & Soc’y 454 (2019).; Molas-Gallart, *supra note* 13, at 367–368; Jay Stowsky, From Spin-Off to Spin-On: Redefining the Military’s Role in Technology Development 36–37 (2005). [↑](#footnote-ref-30)
30. Linda Brandt, Defense Conversion and Dual‐Use Technology: The Push Toward Civil‐Military Integration, 22 POL’Y STUD. J. 359, 360 (1994). [↑](#footnote-ref-31)
31. Michael Brzoska, *Trends in Global Military and Civilian Research and Development (R&D) and Their Changing Interface*, in Proceedings of the International Seminar on Defence Finance and Economics 19, 23 (2006). [↑](#footnote-ref-32)
32. Brandt, supra note 30, at 360; Alic, supra note 14, at 73. [↑](#footnote-ref-33)
33. Sizeable commercial aircraft like the Boeing 707 and 767, or the Airbus A330, originally built for the commercial market, have been adapted for military roles such as airborne early warning, transport, aerial tankers, and surveillance. Commercial jet engines are frequently used to power military aircraft, like the Pratt & Whitney PW2000 turbofan in the C-17 cargo plane. Militaries also widely employ helicopters, trucks, software, and commercial satellite imagery; for more information, see: Id., at 23. [↑](#footnote-ref-34)
34. Office of Technology Assessment, Assessing the Potential for Civil-Military Integration: Selected Case Studies 33 (1995). [↑](#footnote-ref-35)
35. Karen Yeung & Sofia Ranchordás, Introduction, in*An Introduction to Law and Regulation: Text and Materials* 1, 5–6 (Cambridge Univ. Press 2024). [↑](#footnote-ref-36)
36. OECD, The Governance of Regulators, OECD Best Practice Principles for Regulatory Policy (2014), <https://www.oecd.org/en/publications/the-governance-of-regulators_9789264209015-en.html>. [↑](#footnote-ref-37)
37. Machiko Kanetake, Balancing Innovation, Development, and Security: Dual-Use Concepts in Export Control Laws, in *Global Environmental Change and Innovation in International Law* 180-200 (Nicolás Craik, Cameron S.G. Jefferies, Sara L. Seck & Tim Stephens eds., Cambridge Univ. Press 2018).; Paulo Carvão et al., *Governance at a Crossroads: Artificial Intelligence and the Future of Innovation in America*, M-Rcbg Associate Working Paper Series No. 2025.251, Harv. Univ., Cambridge, Ma 36-38 (Feb. 2025); Sofia Ranchordás, *Innovation-Friendly Regulation: The Sunset of Regulation, the Sunrise of Innovation*, 55 Jurimetrics J. 201, 202–03 (2014); Anna Butenko & Pierre Larouche, *Regulation for Innovativeness or Regulation of Innovation?*, 7 Law Innov Technol 52, 57 (2015). [↑](#footnote-ref-38)
38. Anthea Roberts, Henrique Choer Moraes & Victor Ferguson, *Toward a Geoeconomic Order in International Trade and Investment*, 22 J. Int’l Econ. L. 655, 656-657 (2019), <https://doi.org/10.1093/jiel/jgz036>. [↑](#footnote-ref-39)
39. Id. [↑](#footnote-ref-40)
40. Id., at 657. [↑](#footnote-ref-41)
41. Alexandra H. Katich, *Innovation Worth Sharing: Seeking Balance Between Innovation Policy and National Security*, 23 Cardozo J. Int’l & Comp. L. 413, 415 (2015). [↑](#footnote-ref-42)
42. Alic, supra note 14, at 78. [↑](#footnote-ref-43)
43. Katich, *supra note* 41, at 416; Heidi L. Williams, *Intellectual Property Rights and Innovation: Evidence from the Human Genome*, 121 J. Pol. Econ. 1 (2013). [↑](#footnote-ref-44)
44. Brenda M. Simon, Patents, *Information, and Innovation*, 85 Brook. L. Rev. 727, 735–36 (2019). [↑](#footnote-ref-45)
45. The US Constitution states: "promote the progress of science and useful arts". See U.S. CONST. art. I, § 8, cl. 8. [↑](#footnote-ref-46)
46. James Maune, *Patent Secrecy Orders: Fairness Issues in Application of Invention of Secrecy Act,* 20 Tex. Intell. Prop. L.J. 471, 473 (2012). [↑](#footnote-ref-47)
47. *Id.* [↑](#footnote-ref-48)
48. Patents Act 1977, c. 37, § 55-59; Protocol on the Privileges and Immunities of the European Union, arts. 20–21, Oct. 26, 2012, 2012 O.J. (C 326) 266; European Patent Office, Guidelines for Examination in the European Patent Office (Apr. 2010); European Patent Office, Case Law of the Boards of Appeal of the European Patent Office (July 2010). [↑](#footnote-ref-49)
49. Stowsky, supra note 29, at 23. [↑](#footnote-ref-50)
50. Id. [↑](#footnote-ref-51)
51. Peter K Yu, *War and IP*, 49 Brigh Young Univ Law Rev 823, 854-55 (2024). [↑](#footnote-ref-52)
52. **Doni Bloomfield,** Intellectual Antiproperty: Export Controls and the Transformation of IP (unpublished draft, on file with the author). [↑](#footnote-ref-53)
53. Joerg Baten, Nicola Bianchi & Petra Moser, Compulsory Licensing and Innovation—Historical Evidence from German Patents After WWI, 126 J. Dev. Econ. 231, 232 (2017). [↑](#footnote-ref-54)
54. Philippe Aghion et al., Patent Rights, Product Market Reforms, and Innovation, 20 J. Econ. Growth 223, 230-243 (2015). [↑](#footnote-ref-55)
55. Charles Duan, Of Monopolies and Monocultures: The Intersection of Patents and National Security, 36 Santa Clara High Tech. L.J. 369, 399–400 (2020). [↑](#footnote-ref-56)
56. Robert M. Farley, Patents for Power: Intellectual Property and the Diffusion of Military Technology 102 (Davida H. Isaacs ed., 2020). [↑](#footnote-ref-57)
57. *Id.*, at 102-103. [↑](#footnote-ref-58)
58. Rita Matulionytė, Transparency of Facial Recognition Technology and Trade Secrets, in The Cambridge Handbook of Facial Recognition in the Modern State 60–73, 68 (Rita Matulionytė & Monika Zalnieriute eds., 1st ed. 2024). [↑](#footnote-ref-59)
59. *Id.*, at 68-69. [↑](#footnote-ref-60)
60. Tanya Aplin, Reverse Engineering and Commercial Secrets, 66 Current Legal Probs. 341 (2013). [↑](#footnote-ref-61)
61. Matulionytė, *supra* note 58, at 68. [↑](#footnote-ref-62)
62. Hannah Bloch-Wehba, Algorithmic Governance from the Bottom Up, 48 BYU L. Rev. 69, 113-114 (2022). [↑](#footnote-ref-63)
63. Brennan Ctr. for Justice at N.Y. Univ. Sch. of Law v. N.Y.C. Police Dep't, 2017 N.Y. Slip Op. 32716(U) (Sup. Ct. 2017). [↑](#footnote-ref-64)
64. Daniel J. Hemel & Lisa Larrimore Ouellette, Innovation Policy Pluralism, 128 Yale L.J. 544, 551–52 (2019); Joseph E. Stiglitz, Economic Foundations of Intellectual Property Rights, 57 Duke L.J. 1693, 1721 (2008); for instances in Europe and Japan see Alic, supra note 14, at 49-50. [↑](#footnote-ref-65)
65. Hemel & Ouellette, *supra* note 64, at 551. [↑](#footnote-ref-66)
66. I.R.C. §§ 41, 174 (2018) [↑](#footnote-ref-67)
67. Hemel & Ouellette, *supra* note 64, at 552. [↑](#footnote-ref-68)
68. CHIPS Act of 2022, § 102, Pub. L. No. 117-167, 136 Stat. 1366, 1372–73 (2022). [↑](#footnote-ref-69)
69. Aziz Z. Huq, *The Geopolitics of Digital Regulation*, 23 Univ. of Chi. Pub. L. Working Paper 23-24 (2024), [https://ssrn.com/abstract=4946481](https://ssrn.com/abstract%3D4946481) [↑](#footnote-ref-70)
70. Jeremy M. Sharp, U.S. Foreign Aid to Israel, Cong. Rsch. Serv., at 4 (Mar. 1, 2023), <https://sgp.fas.org/crs/mideast/RL33222.pdf> [↑](#footnote-ref-71)
71. *Id.* [↑](#footnote-ref-72)
72. While privacy laws can also serve as tools to mitigate innovation risks, this analysis focuses on national security measures, including patent secrecy, export controls, and restrictions on defense-related technologies. [↑](#footnote-ref-73)
73. Yeung & Ranchordás, supra note 35, at 60-61 [↑](#footnote-ref-74)
74. Id., at 60-61. [↑](#footnote-ref-75)
75. Cindy Whang, *Trade and Emerging Technologies: A Comparative Analysis of the United States and the European Union Dual-Use Export Control Regulations*, 31 SEC. & HUM. RTS. 11, 14-20 (2021). [↑](#footnote-ref-76)
76. Kanetake, supra note 37, at 184-186. [↑](#footnote-ref-77)
77. 35 U.S.C. § 181 (2012). [↑](#footnote-ref-78)
78. Id. [↑](#footnote-ref-79)
79. Id. [↑](#footnote-ref-80)
80. Katich, *supra note* 41, at 417; 35 U.S.C. § 184 (2012). [↑](#footnote-ref-81)
81. 35 U.S.C. § 182 (2012). [↑](#footnote-ref-82)
82. Patents Act 1977 c.37. [↑](#footnote-ref-83)
83. Id. [↑](#footnote-ref-84)
84. Addressing the Threat Posed by TikTok, Exec. Order No. 13942, 85 Fed. Reg. 48637, 48637 (Aug. 6, 2020); Madison Clausius, *The Banning of TikTok, and the Ban of Foreign Software for National Security Purposes*, 21 Wash. U. Global Stud. L. Rev. 273 (2022). [↑](#footnote-ref-85)
85. Protecting Americans’ Sensitive Data From Foreign Adversaries, Exec. Order No. 14034, 86 Fed. Reg. 31423, 31423 (June 9, 2021); Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6,2020). [↑](#footnote-ref-86)
86. the Protecting Americans’ Data from Foreign Adversaries Act of 2024, Pub. L. No. 118-50, div. I (2024). [↑](#footnote-ref-87)
87. The term “controlled by a foreign adversary” means a “covered company or other entity” that is: (A) a foreign person that is domiciled in, is headquartered in, has its principal place of business in, or is organized under the laws of a foreign adversary country; (B) an entity with respect to which a foreign person or combination of foreign persons described in subparagraph (A) directly or indirectly own at least a 20 percent stake; or (C) a person subject to the direction or control of a foreign person or entity described in subparagraph (A) or (B). [↑](#footnote-ref-88)
88. the Protecting Americans’ Data from Foreign Adversaries Act of 2024. [↑](#footnote-ref-89)
89. TikTok Inc. v. Garland, No. 24-1113 (D.C. Cir. 2024). [↑](#footnote-ref-90)
90. Aynne Kokas, Trafficking Data: How China is Winning The Battle For Digital Sovereignty 60 (2023). [↑](#footnote-ref-91)
91. Duan, *supra* note 55, at 380. [↑](#footnote-ref-92)
92. Theodore H. Moran, CFIUS and National Security: Challenges for the United States, Opportunities for the European Union, 19 Peterson Inst. for Int’l Econ. (2017); Theodore Bruckbauer, CFIUS and A.I.: Defending National Security While Allowing Foreign Investment, 4 Geo. L. Tech. Rev. 179, 280–81 (2019); James K. Jackson, The Committee on Foreign Investment in the United States (CFIUS), Cong. Research Serv., 1 (2018). [↑](#footnote-ref-93)
93. Mailyn Fidler, *Zero Progress on Zero Days: How the Last Ten Years Created the Modern Spyware Market*, 103 Neb. L. Rev. 713, 715–16 (2024); Julian J. Koplin, *Dual-Use Implications of AI Text Generation*, 25 Ethics Inf. Technol. 32 (2023). [↑](#footnote-ref-94)
94. Whang, *supra note* 75, at 4-5. [↑](#footnote-ref-95)
95. Id. [↑](#footnote-ref-96)
96. Whang, *supra note* 75, at 25-26. [↑](#footnote-ref-97)
97. Fidler, *supra note* 93 at 715-716, 724-725, 737-738. [↑](#footnote-ref-98)
98. The Wassenar Arrangement on Export Controls of Conventional Arms and Dual-Use Goods and Technologies, Jul. 11-12, .1996, as amended on Dec. 6-7 2000 December 2001. [↑](#footnote-ref-99)
99. Min Xu, *Jeanne M. David & Suk Hi Kim, The Fourth Industrial Revolution: Opportunities and Challenges*, 9 Int’l J. Fin. Res. 90, 380 (2018). [↑](#footnote-ref-100)
100. *Id.* [↑](#footnote-ref-101)
101. O. L. van Daalen, J. V. J. van Hoboken & M. Rucz, *Export Control of Cybersurveillance Items in the New Dual-Use Regulation: The Challenges of Applying Human Rights Logic to Export Control*, 48 Comput. L. & Sec. Rev. 105789 (2023); Thea Riebe et al., *U.S. Security Policy: The Dual-Use Regulation of Cryptography and Its Effects on Surveillance*, 7 Eur. J. for Sec. Rsch. 39 (2022); Machiko Kanetake, The EU’s Dual-Use Export Control and Human Rights Risks: The Case of Cyber Surveillance Technology, 3 Eur. & World: L. Rev. (2019). [↑](#footnote-ref-102)
102. Xu, David, and Kim, *supra note* 99, at 380. [↑](#footnote-ref-103)
103. Lena Riecke, *Unmasking the Term “Dual Use” in EU Spyware Export Control*, 34 Eur. J. Int’l L. 697 (2023); Regulation 2021/821, of the European Parliament and of the Council of 20 May 2021, Setting Up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items, 2021 O.J. (L 206) 1 (EU); Van Daalen, Van Hoboken & Rucz, *supra note* 101. [↑](#footnote-ref-104)
104. Regulation 2021/821, art. 2(1) & 2(20), 2021 O.J. (L 206) 1 (EU). [↑](#footnote-ref-105)
105. János Székely, Legal Aspects of Dual-Use Technologies: Emerging and Disruptive Technologies, in Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment 309, 328–29 (Katarzyna Zombory & János Ede Szilágyi eds., Miskolc-Budapest: Cent. Eur. Acad. Publ’g 2024). [↑](#footnote-ref-106)
106. Doni Bloomfield, *Export Controls and Artificial Intelligence Biosecurity Risks*, SSRN Elec. J. 4 (2024). [↑](#footnote-ref-107)
107. 22 C.F.R. §§ 120.14(a), 120.31, 120.32. [↑](#footnote-ref-108)
108. EAR, 15 CFR. 730ff; ECRA contains the Export Controls Act of 2018 (ECA) and the Anti-Boycott Act of 2018; EAR, Sections 730.6, 742.15. [↑](#footnote-ref-109)
109. See Information Security Controls: Cybersecurity Items, 86 Fed. Reg. 58205 (Oct. 21,2021); 15 C.F.R § 774 Supp. 1 (2024); Exec. Order No. 14093, 88 Fed. Reg. 18957 (Mar. 27, 2023). [↑](#footnote-ref-110)
110. Section 705 of Defense Production Act authorizes the President to “obtain extensive information from private industries” in order to advance national defense interests. 50 U.S.C. § 4555(a); Henry Farrell & ABRAHAM Newman, Underground Empire: How America Weaponized the World Economy 2 (2023), at 102. [↑](#footnote-ref-111)
111. Huq, *supra note* 69, at 18; Farrell & Newman, supra note 110, at 169. [↑](#footnote-ref-112)
112. 50 U.S.C. § 4801 (2018). [↑](#footnote-ref-113)
113. Whang, *supra note* 75, at 25-30. [↑](#footnote-ref-114)
114. Bureau of Industry and Security, Interim Final Rule, 87 Fed. Reg. 62,186 (Oct. 13, 2022). [↑](#footnote-ref-115)
115. Nury Turkel, *AI, National Security, and the Global Technology Race: How US Export Controls Define the Future of Innovation* (2025), Hudson Inst., <https://www.hudson.org/national-security-defense/ai-national-security-global-technology-race-how-us-export-controls-define-nury-turkel>. [↑](#footnote-ref-116)
116. 90 Fed. Reg. 4544 (Jan. 15, 2025). [↑](#footnote-ref-117)
117. Id. [↑](#footnote-ref-118)
118. Turkel, *supra note* 115. [↑](#footnote-ref-119)
119. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3, art. 36. [↑](#footnote-ref-120)
120. Yuval Shany & Tal Mimran, Integrating Privacy Concerns in the Development and Introduction of New Military or Dual Use Technologies, in Rights to Privacy and Data Protection in Times of Armed Conflict5–7 (Asaf Lubin & Russell Buchan eds., CCDCOE 2022), Hebrew Univ. of Jerusalem Int’l L. Forum Working Paper No. 06-21, Hebrew Univ. of Jerusalem Legal Research Paper No. 22-3. [↑](#footnote-ref-121)
121. Audrey Kurth Cronin, How Private Tech Companies Are Reshaping Great Power Competition (Aug. 2023), <https://sais.jhu.edu/kissinger/programs-and-projects/kissinger-center-papers/how-private-tech-companies-are-reshaping-great-power-competition>. [↑](#footnote-ref-122)
122. Anu Bradford, Digital Empires: The Global Battle to Regulate Technology (2023). [↑](#footnote-ref-123)
123. Id., at 33. [↑](#footnote-ref-124)
124. Huq, *supra note* 69. [↑](#footnote-ref-125)
125. Bradford, supra note 122, at 33. [↑](#footnote-ref-126)
126. Id., at 69. [↑](#footnote-ref-127)
127. Kokas, supra note 90, at 18. [↑](#footnote-ref-128)
128. Id., at 60. [↑](#footnote-ref-129)
129. Id., at 3-4, 19. [↑](#footnote-ref-130)
130. Bradford, supra note 122, at 71-72. [↑](#footnote-ref-131)
131. Lance Y. Hunter et al., *The Military Application of Artificial Intelligence Technology* in the United States, China, and Russia and the Implications for Global Security, 39 Def. & Sec. Analysis 207, 226–27 (2023). [↑](#footnote-ref-132)
132. Bradford, *supra note* 122, at 105–06. [↑](#footnote-ref-133)
133. Id., at 9. [↑](#footnote-ref-134)
134. See chapter 2.4. [↑](#footnote-ref-135)
135. Huq, *supra note* 69, at 21. [↑](#footnote-ref-136)
136. István Szabadföldi, *Artificial Intelligence in Military Application – Opportunities and Challenges*, 26 Land Forces Acad. Rev. 157, 157–58 (2021). [↑](#footnote-ref-137)
137. **Congressional Research Service,** Artificial Intelligence and National Security, R45178, at 2 (2020), <https://crsreports.congress.gov>. [↑](#footnote-ref-138)
138. **Jonas Schuett,** Defining the Scope of AI Regulations, 15 Law, Innovation & Tech. 60, 61–62, 66 (2023); Szabadföldi, *supra note* 136, at 158-59*.* [↑](#footnote-ref-139)
139. Mark A. Lemley, Matthew Wansley & David McGowan, *Coopting Disruption*, Cardozo Legal Stud. Res. Paper No. 2024-24, Stan. L. & Econ. Olin Working Paper No. 589, at 37–38 (Feb. 1, 2024), [https://ssrn.com/abstract=4713845](https://ssrn.com/abstract%3D4713845); Fernando van der Vlist, Anne Helmond & Fabian Ferrari, *Big AI: Cloud Infrastructure Dependence and the Industrialisation of Artificial Intelligence*, 11 Big Data & Soc’y, at 3 (2024), https://doi.org/10.1177/20539517241232630. [↑](#footnote-ref-140)
140. Schmid et al., *Arms Race or Innovation Race? Geopolitical AI Development*, Geopolitics, at 2 (2025), <https://doi.org/10.1080/14650045.2025.2456019>. [↑](#footnote-ref-141)
141. Trevor Taylor, *Artificial Intelligence in Defense*, 164 RUSI J. 72, 73 (2019); Roxana Mihet, Rishabh Kumar & Orlando Gomes, *Is It AI or Data That Drives Market Power?*, Swiss Fin. Inst. Res. Paper No. 25-37, 2 (Mar. 31, 2025), [https://ssrn.com/abstract=5199122](https://ssrn.com/abstract%3D5199122); Yavar Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, 31 Harv. J.L. & Tech. 890, 899-900 (2018). [↑](#footnote-ref-142)
142. **Kaushik Kumar Patel,** Ethical Reflections on Data-Centric AI: Balancing Benefits and Risks, 2 Int’l J. Artif. Intell. Res. & Dev. 1, 4–5 (2024);Niva Elkin-Koren & Michal S. Gal, *The Chilling of Governance-by-Data on Data Markets*, 86 U. Chi. L. Rev. 403, 428-29 (2019). [↑](#footnote-ref-143)
143. Lucrezia Fanti, Dario Guarascio & Massimo Moggi, From Heron of Alexandria to Amazon’s Alexa: A Stylized History of AI and Its Impact on Business Models, Organization and Work, 49 J. INDUS. & BUS. ECON. 409, 420 (2022); See a broader discussion of this topic in Chapter 4.2.2 of the research proposal. [↑](#footnote-ref-144)
144. van der Vlist, *supra note* 139, at 13; Thomas A. Hemphill, US AI Data Centers and Deployment Challenges for Small Modular Reactors: Proposed Regulatory Policy Recommendations, 51 Sci. & Pub. Pol’y 999 (2024), <https://doi.org/10.1093/scipol/scae040>; Huixiang Li et al., *AI Face Recognition and Processing Technology Based on GPU Computing*, 4 J. Theory & Prac. Eng’g Sci. 9 (2024); Lauren Leffer, *The AI Boom Could Use a Shocking Amount of Electricity*, Sci. Am. (Oct. 13, 2023), <https://www.scientificamerican.com/article/the-ai-boom-could-use-a-shocking-amount-of-electricity/>; Ariel Cohen, *AI is Pushing the World Toward an Energy Crisis*, Forbes (May 24, 2024), <https://www.forbes.com/sites/arielcohen/2024/05/23/ai-is-pushing-the-world-towards-an-energy-crisis/>;Huq, *supra note* 69, at 41-42. [↑](#footnote-ref-145)
145. Kelley M. Sayler & Daniel S. Hoadley, *Artificial Intelligence and National Security*, Cong. Rsch. Serv. 2 (2020). [↑](#footnote-ref-146)
146. Szabadföldi, *supra note* 136, at 158. [↑](#footnote-ref-147)
147. Bathaee, *supra note* 141, at 901-902; Bernard Marr, *What Is Deep Learning AI? A Simple Guide with 8 Practical Examples*, Forbes (2021). [↑](#footnote-ref-148)
148. **Congressional Research Service,** *supra note* 137, at 2-3. [↑](#footnote-ref-149)
149. Magdalena Pacholska, *Many Hands in the Black Box: Artificial Intelligence and the Responsibility of International Organizations* 2 (T.M.C. Asser Inst. for Int’l & Eur. L., Asser Rsch. Paper 2023-04, 2023), forthcoming in Reassessing the Articles on the Responsibility of International Organizations: From Theory to Practice (Rossana Deplano, Antal Berkes & Richard Collins eds., Edward Elgar Publ’g 2023), available at https://ssrn.com/abstract=4501072. [↑](#footnote-ref-150)
150. Bathaee, *supra note* 141, at 901. [↑](#footnote-ref-151)
151. *U.S. Gov’t Accountability Off.,* *Artificial Intelligence: DOD Needs Department-Wide Guidance to Inform Acquisitions* (2023), <https://www.gao.gov/assets/gao-23-105850.pdf>; Jan Maarten Schraagen, *Responsible Use of AI in Military Systems: Prospects and Challenges*, 66 Ergonomics 1719, 1720 (2023); Ashley Deeks, Noam Lubell & Daragh Murray, *Machine Learning, Artificial Intelligence, and the Use of Force by States*, 10 J. Nat’l Sec. L. & Pol’y 1 (2019). [↑](#footnote-ref-152)
152. Sayler & Hoadley *supra note* 145, at 9-15. [↑](#footnote-ref-153)
153. Omar Yousef Shehabi & Asaf Lubin, *Israel – Hamas 2024 Symposium – Algorithms of War: Military AI and the War in Gaza*, Lieber Inst. West Point (2024); Jan Maarten Schraagen, *Introduction to Responsible Use of AI in Military Systems*, in Responsible Use of AI in Military Systems 3, 3–4 (Jan Maarten Schraagen ed., Taylor & Francis 2024); Jean-Marc Rickli & Federico Mantellassi, *Artificial Intelligence in Warfare: Military Uses of AI and Their International Security Implications*, in The AI Wave in Defence Innovation 12, 12–36 (Routledge 2023). [↑](#footnote-ref-154)
154. In 2018, Israel was awarded the Prime Minister's Award to the General Security Service for a machine learning-based project that helped solve hundreds of attacks based on analyzing information from various sources. For more information, see Yoav Zeyton & Itamar Eichner, 500 Failures a Year: Netanyahu and the Head of the Shin Bet Awarded a Prize to Groundbreaking Operations, Ynet (2018), <https://www.ynet.co.il/article/5420482>. [↑](#footnote-ref-155)
155. Gibbs Samuel, *Google’s AI Is Being Used by US Military Drone Programme*, The Guardian (2018). [↑](#footnote-ref-156)
156. Bloch-Wehba, *supra* *note* 62, at 93-94. [↑](#footnote-ref-157)
157. Ewa Jasiuk, Anna Chochowska & Krzysztof Chochowski, *Legal Dilemmas of Drone Development in Poland*, 110 J. Intell. Robot. Syst. 78, 2-3 (2024); Saba Sotoudehfar & Jeremy Julian Sarkin, *Drones on the Frontline: Charting the Use of Drones in the Russo-Ukrainian Conflict and How Their Use May Be Violating International Humanitarian Law,* 23 Int’l & Comp. L. Rev. 129, 131-33 (2023); Marc R. DeVore, *“No End of a Lesson:” Observations from the First High-Intensity Drone War,* 39 Def. & Sec. Analysis 263 (2023); **Alyssa Sims,** The Rising Drone Threat from Terrorists, 19 Geo. J. Int'l Aff. 97, 99–100 (2018). [↑](#footnote-ref-158)
158. Shehabi & Lubin, *supra note* 153; Qingtian Wu & Yimin Zhou, Real-Time Object Detection Based on Unmanned Aerial Vehicle (2019); Adib Bin Rashid et al., *Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges*, 2023 Int’l J. Intelligent Sys. 1, 4 (2023). [↑](#footnote-ref-159)
159. מענה דובר צה"ל לבקשת חופש המידע מטעם האגודה לזכויות האזרח בישראל "לבחון את השימוש במערכת "הבשורה" המשמשת להצעת מטרות לתקיפה צבאית" **דובר צה״ל** (20.2.2024), . [↑](#footnote-ref-160)
160. Israel Defense Forces, The IDF’s Use of Data Technologies in Intelligence Processing, Press Release (June 18, 2024), <https://www.idf.il/en/mini-sites/idf-press-releases-israel-at-war/june-24-pr/the-idf-s-use-of-data-technologies-in-intelligence-processing/> (Hereinafter: "IDF Press Release"); Elizabeth Dwoskin, Israel Built an ‘AI Factory’ for War. It Unleashed It in Gaza, Wash. Post (Dec. 29, 2024), <https://www.washingtonpost.com/technology/2024/12/29/ai-israel-war-gaza-idf/>; Gaby Del Valle, *Report: Israel Used AI to Identify Bombing Targets in Gaza*, The Verge (Apr. 4, 2024), <https://www.theverge.com/2024/4/4/24120352/israel-lavender-artificial-intelligence-gaza-ai>. [↑](#footnote-ref-161)
161. ינון שלום יתח "ב-8200 פיתחו מערכת שיודעת לזהות פיגועים – עוד לפני שקרו" **אתר צה"ל** (2021); Gautam Ramachandra, How Artificial Intelligence is Improving Iron Dome, Medium (May 13, 2023), [https://medium.com/@gautamrbharadwaj/how-ai-is-improving-iron-dome-3894cd3668f9](https://medium.com/%40gautamrbharadwaj/how-ai-is-improving-iron-dome-3894cd3668f9); Rashid et al., *supra* *note* 158, at 4. [↑](#footnote-ref-162)
162. Schmid, *supra note* 140, at 1. [↑](#footnote-ref-163)
163. Tania Babina et al*., Artificial Intelligence, Firm Growth, and Product Innovation*, 151 J. Fin. Econ. 103745, 4 (2024); Efraim Benmelech & Michal Zator, *Robots and Firm Investment*, Nat’l Bureau of Econ. Research, Working Paper No. 29676, at 11–13 (2022); Roxana Mihet & Thomas Philippon, *The Economics of Big Data and Artificial Intelligence, in Disruptive Innovation in Business and Finance* in the Digital World 20, 29, 30–32 (2019); Ingvild Bode, Cecilia Ducci & Pak K. Lee*, Narrating and Practising the US–China “Tech War,”* 5 Global Stud. Q. (Apr. 2025), <https://doi.org/10.1093/isagsq/ksaf037>.; Hunter et al., *supra note* 131, at 226. [↑](#footnote-ref-164)
164. Schmid, *supra note* 140, at 2-3. [↑](#footnote-ref-165)
165. Id., at 10-11. [↑](#footnote-ref-166)
166. Shaleen Khanal, Hongzhou Zhang & Araz Taeihagh, *Development of New Generation of Artificial Intelligence in China: When Beijing’s Global Ambitions Meet Local Realities*, 34 J. Contemp. China 19, 19–20 (2025), <https://doi.org/10.1080/10670564.2024.2333492>; Richard A. Bitzinger & Michael Raska, *Chinese and Russian Military Modernization and the Fourth Industrial Revolution*, in Russia-China Relations 121, 124–28 (Alice Kirchberger, Sinjen Kirchberger & Kai Wörmer eds., 2022). [↑](#footnote-ref-167)
167. Yunfei Xing, Wu He, Justin Zuopeng Zhang & Gaohui Cao, *AI Privacy Opinions between US and Chinese People*, 63 J. Comput. Info. Sys. 492, 500 (2022), https://doi.org/10.1080/08874417.2022.2079107. [↑](#footnote-ref-168)
168. Hunter et al., *supra note* 131, at 227. [↑](#footnote-ref-169)
169. Jim Mattis, Summary of the 2018 National Defense Strategy of the United States of America, U.S. Dep’t of Def. (2018), <https://apps.dtic.mil/sti/citations/AD1045785>. [↑](#footnote-ref-170)
170. *Artificial Intelligence for the American People*, White House (2019), https://trumpwhitehouse.archives.gov/ai/. [↑](#footnote-ref-171)
171. Denise Garcia, *Stop the Emerging AI Cold War*, 593 Nature 169 (2021); Michèle A. Flournoy, *AI Is Already at War*, 102 Foreign Aff. 56 (2023). [↑](#footnote-ref-172)
172. Regulation 2024/1689, of the European Parliament and of the Council of 9 October 2024 on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 268) 1; Schmid, *supra note* 140, at 10-11. [↑](#footnote-ref-173)
173. See Chapter 2.2. [↑](#footnote-ref-174)
174. Sebastian Clapp, *Defence and Artificial Intelligence*, Eur. Parl. Res. Serv., PE 569.580 (Apr. 2025), [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS\_BRI(2025)769580\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI%282025%29769580_EN.pdf). [↑](#footnote-ref-175)
175. Bitzinger, *supra note* 166, at 17-18; **Jake Sullivan,** Remarks by APNSA Jake Sullivan on AI and National Security, The White House (Oct. 24, 2024), <https://www.whitehouse.gov/briefing-room/speeches-remarks/2024/10/24/remarks-by-apnsa-jake-sullivan-on-ai-and-national-security/> ("Private companies are leading the development of AI, not the government."); Cronin, *supra note* 121; Nir Reuven & Eitan Shamir, The Shift in Technological Dominance and the Adaption of Open Innovation by the Defence Sector, Def. & Sec. Analysis, at 14 (Apr. 3, 2025), <https://doi.org/10.1080/14751798.2025.2484920>. [↑](#footnote-ref-176)
176. Barry Pavel et al., *AI and Geopolitics: How Might AI Affect the Rise and Fall of Nations?* RAND Corp. (2023), <https://www.rand.org/pubs/perspectives/PEA3034-1.html>. [↑](#footnote-ref-177)
177. Cronin, *supra note* 121. [↑](#footnote-ref-178)
178. Bitzinger, *supra note* 166, at 14-19. [↑](#footnote-ref-179)
179. Jeff White, Council Post: Why Public-Private Collaboration Is Critical to Our Future in Tech, Forbes (Oct. 20, 2023), <https://www.forbes.com/councils/forbestechcouncil/2023/10/20/why-public-private-collaboration-is-critical-to-our-future-in-tech/>; J. White, *Council Post: Why Public-Private Collaboration Is Critical to Our Future in Tech*, Forbes (2023). [↑](#footnote-ref-180)
180. **Joshua Glonek,** The Coming Military AI Revolution, Mil. Rev. (2024), at 88, 97-98, <https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/May-June-2024/MJ-24-Glonek/MJ-24-Glonek-UA.pdf>. [↑](#footnote-ref-181)
181. Lemley, supra note 139, at 10. [↑](#footnote-ref-182)
182. Kokas, supra note 90, at 94. [↑](#footnote-ref-183)
183. Lemley, supra note 139, at 11; Shaleen Khanal, Hongzhou Zhang & Araz Taeihagh, *Why and How Is the Power of Big Tech Increasing in the Policy Process? The Case of Generative AI*, 44 Pol’y & Soc’y 52, 53 (2025). [↑](#footnote-ref-184)
184. Lemley, supra note 139, at 22; Coveri 2024, supra note 6, at 6-7; Khanal, *supra note* 183, at 53-54. [↑](#footnote-ref-185)
185. S. Rolf & S. Schindler, The US–China Rivalry and the Emergence of State Platform Capitalism, 55 Env’t & Plan. A: Econ. & Space 1255 (2023). [↑](#footnote-ref-186)
186. Kokas, supra note 90, at 2. [↑](#footnote-ref-187)
187. Sebastián Fernández Franco et al., *Producing and Using Artificial Intelligence: What Can Europe Learn from Siemens’s Experience?*, 27 COMPETITION & CHANGE 302 (2022), <https://doi.org/10.1177/10245294221097066>. [↑](#footnote-ref-188)
188. Vera Bergengruen, Ukraine’s “Secret Weapon” Against Russia Is Clearview AI, Time (2023), https://time.com/6334176/ukraine-clearview-ai-russia/. [↑](#footnote-ref-189)
189. Coveri 2024, supra note 6, at 17-18. [↑](#footnote-ref-190)
190. Id. [↑](#footnote-ref-191)
191. Franco, *supra note* 187. [↑](#footnote-ref-192)
192. Id. [↑](#footnote-ref-193)
193. Id. [↑](#footnote-ref-194)
194. *See* for e.x. the U.s investment in Military application of AI: **U.S. Gov’t Accountability Off.,** Artificial Intelligence: DOD Needs Department-Wide Guidance to Inform Acquisitions (2023), <https://www.gao.gov/assets/gao-23-105850.pdf> [↑](#footnote-ref-195)
195. Lemley, supra note 139, at 38-41; van der Vlist, *supra note* 139, at 5. [↑](#footnote-ref-196)
196. Id. [↑](#footnote-ref-197)
197. **Glonek**, *supra note* 180, at 92-93. [↑](#footnote-ref-198)
198. Coveri 2024, supra note 6, at 21; van der Vlist, *supra note* 139, at 5-6. [↑](#footnote-ref-199)
199. Id, at 12. [↑](#footnote-ref-200)
200. Vitaliy Goncharuk, *Survival of the Smartest? Defense AI in Ukraine*, in The Very Long Game: 25 Case Studies on the Global State of Defense AI 375, 384-85 (Springer Nature Switzerland 2024); Anne Sophie Delphin Amdal, *Civilian and Private Actors’ Support of Ukrainian National Resistance*, FFI Norwegian Def. Rsch. Establishment 13-21 (Sept. 16, 2022), https://www.ffi.no/en/publications-archive/civilian-and-private-actors-support-of-ukrainian-national-resistance. [↑](#footnote-ref-201)
201. **Goncharuk, *supra note* 200, at 384–85; See also Chapter 3.6 about the use of FRT applications.** [↑](#footnote-ref-202)
202. Benjamin M. Jensen, Christopher Whyte & Scott Cuomo, *Algorithms at War: The Promise, Peril, and Limits of Artificial Intelligence*, 22 Int’l Stud. Rev. 526, 532 (2020); Kaushik Ray & William Selvamurthy, *Starlink’s Role in Ukraine*, 17 J. Def. Stud. 25 (2023); Walter Isaacson, Elon Musk 456–57 (1st ed. 2023); Josh Pennington & Sean Lyngaas, *Starlink in Use on ‘All Front Lines,’ Ukraine Spy Chief Says, but Wasn’t Active ‘for Time’ over Crimea*, CNN (Sept. 10, 2023), <https://www.cnn.com/2023/09/10/europe/ukraine-starlink-not-active-crimea-intl-hnk/index.html>; Marc Santora, *Surrender to a Drone? Ukraine Is Urging Russian Soldiers to Do Just That*, N.Y. Times (Dec. 20, 2022), https://www.nytimes.com/2022/12/20/world/europe/russian-soldier-drone-surrenders.html; David Hambling, *Drones Killing Without Oversight?*, 260 New Sci. 8 (2023). [↑](#footnote-ref-203)
203. Amritha Jayanti, *Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?*, Belfer Ctr. for Sci. & Int’l Affs., Harv. Kennedy Sch. (2023); Ray & Selvamurthy, *supra note* 202, at 35. [↑](#footnote-ref-204)
204. Roy Lindelauf, Herwin Meerveld & Marie Postma, *Leveraging Decision Support in the Russo-Ukrainian War: The Role of Artificial Intelligence*, 47 Atlantisch Perspectief 36 (2023); Peter Dauvergne, *The Corporate Politics of Facial Recognition*, *in* Identified, Tracked, and Profiled 59 (2022). [↑](#footnote-ref-205)
205. Juan Espindola, *Facial Recognition in War Contexts: Mass Surveillance and Mass Atrocity*, 37 Ethics & Int’l Aff. 177, 179 (2023); Bergengruen 2023, *supra note* 188. [↑](#footnote-ref-206)
206. Paresh Dave & Jeffrey Dastin, *Exclusive: Ukraine Has Started Using Clearview AI’s Facial Recognition*, Reuters (Mar. 14, 2022), https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/. [↑](#footnote-ref-207)
207. Agnė Limantė, *Faces of War: Russia’s Invasion of Ukraine and Military Use of Facial Recognition Technology*, in The Cambridge Handbook of Facial Recognition in the Modern State 112, 112–13 (Rita Matulionytė & Monika Zalnieriute eds., 1st ed. 2024). [↑](#footnote-ref-208)
208. Vera Bergengruen, Tech Companies Turned Ukraine into an AI War Lab, Time (2024), <https://time.com/6691662/ai-ukraine-war-palantir/>; Bruno Maçães, How Palantir Is Shaping the Future of Warfare, Time (2023), <https://time.com/6293398/palantir-future-of-warfare-ukraine/>. [↑](#footnote-ref-209)
209. Bergengruen 2024, *supra* *note* 208. [↑](#footnote-ref-210)
210. Itzhak Aviv & Uri Ferri, *Russian-Ukraine Armed Conflict: Lessons Learned on the Digital Ecosystem*, 43 Int’l J. Critical Infrastructure Prot. 100637 (2023). [↑](#footnote-ref-211)
211. Bergengruen 2024, supra note 208. [↑](#footnote-ref-212)
212. Ron Crissy, *Disaster Brings Israeli AI Breakthrough to Identify the Dead,* Ynet (2024), https://www.ynetnews.com/business/article/sklzlxb5a. [↑](#footnote-ref-213)
213. Shehabi & Lubin, *supra note* 153. [↑](#footnote-ref-214)
214. Assaf Gilead, Defense Ministry to Procure 20,000 Israeli-Made Drones, Globes (Aug. 29, 2024), <https://en.globes.co.il/en/article-idf-to-procure-20000-israeli-made-drones-1001487932>. [↑](#footnote-ref-215)
215. Eyal Boguslavsky, Meet the Rooster, Robotican's New Hybrid Robotic Drone Employed by the IDF in Gaza, Israel Defense (Jan. 18, 2024), <https://www.israeldefense.co.il/en/node/60981>. [↑](#footnote-ref-216)
216. *How XTEND’s AI-Powered Drones Are Saving Lives on the Frontline*, The Defense Post (Oct. 14, 2024), <https://thedefensepost.com/2024/10/14/xtend-drones/>. [↑](#footnote-ref-217)
217. Assaf Gilad, This Is How the Ranks of the Army Were Filled with Drones and Robots Made by Small Israeli Companies, Globes (2024), <https://www.globes.co.il/news/article.aspx?did=1001477095>. [↑](#footnote-ref-218)
218. *Id.* [↑](#footnote-ref-219)
219. Coveri 2025, supra note 6, at 85; Limantė, *supra* *note* 207, 123-24. [↑](#footnote-ref-220)
220. Coveri 2025, supra note 6, at 85. [↑](#footnote-ref-221)
221. Limantė, *supra* *note* 207, 123-24; A similar claim is also made in Wolfgang Streeck, Notes on the Political Economy of War, 12 REV. KEYNESIAN ECON. 293, 296 (Autumn 2024), <https://wolfgangstreeck.com/wp-content/uploads/2024/09/streeck_2024.pdf>. [↑](#footnote-ref-222)
222. *Id.* [↑](#footnote-ref-223)
223. *NATO Acquires AI-Enabled Warfighting System*, NATO (Apr. 14, 2025), <https://shape.nato.int/news-releases/nato-acquires-aienabled-warfighting-system->. [↑](#footnote-ref-224)
224. Bilyana Lilly et al., *Business@War: The IT Companies Helping to Defend Ukraine*, in 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon) (IEEE 2023). [↑](#footnote-ref-225)
225. *Id*. [↑](#footnote-ref-226)
226. Ulrike Franke & Jenny Soederstroem, *Star Tech Enterprise: Emerging Technologies in Russia’s War on Ukraine*, Eur. Council on Foreign Rel. 5 (2023). [↑](#footnote-ref-227)
227. Evan Selinger & Brenda Leong, *The Ethics of Facial Recognition Technology*, in Oxford Handbook of Digital Ethics 590 (2022); Denise Almeida, Konstantin Shmarko & Elizabeth Lomas, *The Ethics of Facial Recognition Technologies, Surveillance, and Accountability in an Age of Artificial Intelligence: A Comparative Analysis of US, EU, and UK Regulatory Frameworks*, 2 AI & Ethics 377, 378 (2022). [↑](#footnote-ref-228)
228. Mailyn Fidler & Justin (Gus) Hurwitz, *An Overview of Facial Recognition Technology Regulation in the United States*, in The Cambridge Handbook of Facial Recognition in the Modern State214, 214–15 (Rita Matulionyte & Monika Zalnieriute eds., 2024). [↑](#footnote-ref-229)
229. Ido Rosenzweig & Magdalena Pacholska, The Use of Facial Recognition for Targeting under International Law, Int'l Rev. Red Cross (forthcoming 2025), available at [https://ssrn.com/abstract=](https://ssrn.com/abstract%3D). [↑](#footnote-ref-230)
230. Gautam Srivastava & Surajit Bag, *Modern-Day Marketing Concepts Based on Face Recognition and Neuro-Marketing: A Review and Future Research Directions*, 31 Benchmarking: An Int’l J. 410, 413 (2024). [↑](#footnote-ref-231)
231. Coveri 2025, supra note 6, at 81. [↑](#footnote-ref-232)
232. Monique Mann & Marcus Smith, *Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight*, 40 UNSW L.J. 121, 122–23 (2017). [↑](#footnote-ref-233)
233. Almeida, *supra note* 227; Madeleine Gregory, Amazon’s Facial Recognition Misidentified 1 in 5 California Lawmakers as Criminals, Vice (Aug. 13, 2019), https://www.vice.com/en\_us/article/ne8wa8/amazons-facial-recognition-misidentified-1-in-5-californialawmakers-as-criminals. [↑](#footnote-ref-234)
234. Agnė Limantė, *Bias in Facial Recognition Technologies Used by Law Enforcement: Understanding the Causes and Searching for a Way Out*, 42 Nordic J. Hum. Rts. 115, 116 (2023); An incident that highlights the risks of relying on inaccurate technology for suspect identification occurred in 2020 during a police investigation in Detroit involving Robert Williams. Williams, an African American man, was arrested for shoplifting based on a facial recognition identification. However, it was later determined that this identification was a false match, relying on his driver’s license photograph and distorted surveillance footage from the crime scene. *See* Marcus Smith & Monique Mann, Facial Recognition Technology and Potential for Bias and Discrimination, in The Cambridge Handbook of Facial Recognition in the Modern State 87, 90 (Rita Matulionytė & Monika Zalnieriute eds., 1st ed. 2024). [↑](#footnote-ref-235)
235. Brian Jefferson, Digitize and Punish: Racial Criminalization in the Digital Age 11 Univ. of Minn. Press (2020). [↑](#footnote-ref-236)
236. Smith & Mann, *supra* *note* 234, at 91-92. [↑](#footnote-ref-237)
237. Several law enforcement agencies reportedly used FRT to identify and arrest individuals accused of violence and property crimes during the George Floyd protests. *See, e.g.* Richland County Sheriff’s Department, Richland, Columbia Police Use Facial Recognition, Social Media in Protest Tied Arrests, The State (Aug. 2, 2020), <https://www.thestate.com/news/local/crime/article244433082.html>; Justin Jouvenal & Spencer S. Hsu, Facial Recognition Used to Identify Lafayette Square Protester Accused of Assault, Wash. Post (Nov. 2, 2020), <https://www.washingtonpost.com/local/legal-issues/facial-recognition-protests-lafayette-square/2020/11/02/64b03286-ec86-11ea-b4bc-3a2098fc73d4_story.html>. [↑](#footnote-ref-238)
238. Bloch-Wehba, *supra* *note* 62, at 100-101. [↑](#footnote-ref-239)
239. Anil Kalhan, *Immigration Surveillance*, 74 Md. L. Rev. 1 (2014). [↑](#footnote-ref-240)
240. Bloch-Wehba, *supra* *note* 62, at 103-104. [↑](#footnote-ref-241)
241. Amitai Ziv, *This Israeli Face-Recognition Startup Is Secretly Tracking Palestinians*, Haaretz (July 15, 2019), <https://www.haaretz.com/israel-news/business/2019-07-15/ty-article/.premium/this-israeli-face-recognition-startup-is-secretly-tracking-palestinians/0000017f-f47b-ddde-abff-fc7fe25c0000>; Omar Yousef Shehabi, *Surveillance, Data Collection and Data Mining in Occupied Territory*, in Rights to Privacy and Data Protection in Times of Armed Conflict (Russell Buchan & Asaf Lubin eds., 2022). [↑](#footnote-ref-242)
242. Elizabeth Dwoskin, *Israel Escalates Surveillance of Palestinians with Facial Recognition Program in West Bank*, Wash. Post (Nov. 5, 2021), https://www.washingtonpost.com/world/middle\_east/israel-palestinians-surveillance-facial-recognition/2021/11/05/3787bf42-26b2-11ec-8739-5cb6aba30a30\_story.html. [↑](#footnote-ref-243)
243. Omar Yousef, *supra note* 241. [↑](#footnote-ref-244)
244. The European Union's Artificial Intelligence Act (EU AI Act) states that collecting facial images from the Internet or CCTV footage to create facial recognition databases poses "unacceptable levels of risk." As a result, this practice is prohibited. See **Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts**, art. 5, COM (2021) 206 final (Apr. 21, 2021). In the United States, at least seven states have implemented some form of a ban on FRT. For more information See Mark Andrejevic & Neil Selwyn, Facial Recognition 74–75 (2022). [↑](#footnote-ref-245)
245. The EU AI Act, for example, doesn't place any restrictions on systems used for military or defense purposes. Furthermore, the law allows law enforcement agencies to use remote biometric identification in public spaces during emergencies, such as searching for victims of kidnapping or human trafficking, preventing specific acts of terrorism, and locating individuals involved in crimes. However, this use is contingent upon the implementation of specified protective measures. For a broader discussion on the EU, see e.x*.* Marko Jurić, *Legal Aspects of Military and Defence Applications of Artificial Intelligence Within the European Union*, in Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment395, 415–16 (K. Zombory & J.E. Szilágyi eds., Miskolc-Budapest: Cent. Eur. Acad. Publ’g 2024); János Székely, *Legal Aspects of Dual-Use Technologies: Emerging and Disruptive Technologies*, in Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment309, 334–35 (Katarzyna Zombory & János Ede Szilágyi eds., Miskolc-Budapest: Cent. Eur. Acad. Publ’g 2024). [↑](#footnote-ref-246)
246. See Chapter 3.3. [↑](#footnote-ref-247)
247. Limantė, supra note 234, at 112. [↑](#footnote-ref-248)
248. *Id.,* at 112-115. [↑](#footnote-ref-249)
249. *Id.*, at 123. [↑](#footnote-ref-250)
250. Thomas Brewster, *Israeli “Cyber War Room” Uses Amazon Facial Recognition to Find Missing and Dead after Hamas Attack*, Forbes (Oct. 20, 2023), https://www.forbes.com/sites/thomasbrewster/2023/10/20/israel-uses-amazon-facial-recognition-to-identify-missing-and-dead-in-hamas-war/. [↑](#footnote-ref-251)
251. Thomas Brewster*, Israel Hospital Uses Facial Recognition to Identify Dead and Wounded from Hamas War*, Forbes (Oct. 11, 2023), https://www.forbes.com/sites/thomasbrewster/2023/10/11/hospital-uses-facial-recognition-to-identify-israel-hamas-war-dead/. [↑](#footnote-ref-252)
252. Sheera Frenkel, Israel Deploys Expansive Facial Recognition Program in Gaza, N.Y. Times (Mar. 27, 2024), <https://www.nytimes.com/2024/03/27/technology/israel-facial-recognition-gaza.html>. [↑](#footnote-ref-253)
253. ***Corsight***, STARTUP NATION FINDER, <https://finder.startupnationcentral.org/company_page/corsight> (last visited May 6, 2025). [↑](#footnote-ref-254)
254. Andrejevic & Selwyn, supra note 244, at 86-88. [↑](#footnote-ref-255)
255. Id. [↑](#footnote-ref-256)
256. Id., 84. [↑](#footnote-ref-257)
257. Id., 91-93. [↑](#footnote-ref-258)
258. Yasmin Afina & Sarah Grand-Clément, Bytes and Battles: Inclusion of Data Governance in Responsible Military AI, CIGI Papers No. 308, at 10 (Oct. 2024), <https://www.cigionline.org/static/documents/Afina-Grand_Clement.pdf> [↑](#footnote-ref-259)
259. ***Corsight***, supra note 253. [↑](#footnote-ref-260)
260. Afina & Grand-Clément, *supra note* 258, at 10. [↑](#footnote-ref-261)
261. Niva Elkin-Koren, Government ‒ Platform Synergy and Its Perils, in CONSTITUTIONALIZING SOCIAL MEDIA 17–18 (B. Celeste, A. Heldt & M. Iglesias eds., Hart Publ’g 2022), [https://ssrn.com/abstract=4292537](https://ssrn.com/abstract%3D4292537). [↑](#footnote-ref-262)
262. Id. [↑](#footnote-ref-263)
263. *New Report on Artificial Intelligence and Related Technologies in Military Decision-Making on the Use of Force in Armed Conflicts*, Geneva Acad. & Int’l Comm. Of The Red Cross 14 (May 13, 2024), <https://www.geneva-academy.ch/news/detail/716-new-report-on-artificial-intelligence-and-related-technologies-in-military-decision-making-on-the-use-of-force-in-armed-conflicts>; Paresh Dave & Jeffrey Dastin, *Ukraine Has Started Using Clearview AI’s Facial Recognition During War*, Reuters (Mar. 14, 2022), <https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/>; Wei Liu & Liyang Hou, *The Legal Boundary of Data Scraping*, 15 Queen Mary J. Intell. Prop*.* 219 (2025). [↑](#footnote-ref-264)
264. Tshilidzi Marwala, *Militarization of AI Has Severe Implications for Global Security and Warfare*, United Nations Univ. (July 24, 2023), <https://unu.edu/article/militarization-ai-has-severe-implications-global-security-and-warfare>. [↑](#footnote-ref-265)
265. See e.x. Michael D. Birnhack and Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 Va J L & Tech 6, 17–28 (2003); Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 Stan L Rev 99, 112–22 (2018); *Developments in the Law: More Data, More Problems,* 131 Harv L Rev 1714, 1729–36 (2018); Niva Elkin-Koren and Eldar Haber, *Governance by Proxy: Cyber Challenges to Civil Liberties*, 82 Brooklyn L Rev 105, 131–43 (2016); Jon D. Michaels, *All the President’s Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 Cal L Rev 901, 929–41 (2008). [↑](#footnote-ref-266)
266. Afina & Grand-Clément, *supra note* 258, at 10; Guillaume Gadek, *Unreliable AIs for the Military*, in Responsible Use of AI in Military Systems 101, 116 (Jan Maarten Schraagen ed., Taylor & Francis 2024). [↑](#footnote-ref-267)
267. Department of Defense Report: State of Competition within the Defense Industrial Base, Office of the Under Secretary of Defense for Acquisition and Sustainment, p. 7 (Feb. 2022), <https://media.defense.gov/2022/feb/15/2002939087/-1/-1/1/state-of-competition-within-the-defense-industrial-base.pdf>; Azza Jayaprakash, Decoding AI Acquisitions and Data Rights, Def. Acquis. Mag., May–June 2024, available at <https://www.dau.edu/library/damag/may-june2024/decoding-ai-acquisitions>. [↑](#footnote-ref-268)
268. Kokas, supra note 90, at 59-60. [↑](#footnote-ref-269)
269. See, for e.x. *the American DoD instruction for Software Acquisition* in **U.S. Dep’t of Def. Instruction 5000.87, Operation of the Software Acquisition Pathway, § 3.2.e IP Strategy** (Oct. 2, 2020), available at <https://www.acq.osd.mil/asda/dpc/api/acquisition-approaches-management.html>; Shyam Sankar, Caitlin Dohrman & Madeline Zimmerman, The Military’s Insistence on Owning Commercial Intellectual Property Is Limiting Innovation (Jan. 16, 2024), <https://warontherocks.com/2024/01/the-militarys-insistence-on-owning-commercial-intellectual-property-is-limiting-innovation/>; Kelley M. Sayler, *Emerging Military Technologies: Background and Issues for Congress* 35, Cong. Rsch. Serv.(2022), available at <https://crsreports.congress.gov>; Sankar, Dohrman & Zimmerman, *supra* *note* 269; Azza Jayaprakash, Decoding AI Acquisitions and Data Rights, Def. Acquis. Mag., May–June 2024, available at <https://www.dau.edu/library/damag/may-june2024/decoding-ai-acquisitions>. [↑](#footnote-ref-270)
270. Tal Mimran, Magdalena Pacholska, Gil Dahan & Lorenzo Trabucco, Israel–Hamas 2024 Symposium–Beyond the Headlines: Combat Deployment of Military AI-Based Systems by the IDF (Feb. 2, 2024), available at <https://pure.uva.nl/ws/files/185398008/lieber.westpoint.edu-Israel_Hamas_2024_Symposium_Beyond_the_Headlines_Combat_Deployment_of_Military_AI-Based_Systems_by_.pdf>. [↑](#footnote-ref-271)
271. Burcu Kilic, Into Uncharted Waters: Trade Secrets Law in the AI Era, CIGI Papers No. 295, 14–15 (2024), available at <https://www.cigionline.org/publications/into-uncharted-waters-trade-secrets-law-in-the-ai-era/>.; **Cary Coglianese,** AI, Due Process, and Trade Secrets, The Regulatory Review (Sept. 4, 2023), https://www.theregreview.org/2023/09/04/coglianese-ai-due-process-and-trade-secrets/. [↑](#footnote-ref-272)
272. **Id.** [↑](#footnote-ref-273)
273. **Royal Brush Mfg., Inc. v. United States,** No. 2022-1226, slip op. at 12-13 (Fed. Cir. July 27, 2023). [↑](#footnote-ref-274)
274. **Lauren Sanders,** Australia’s Defense Export Control Regime and Critical Technologies, J. Strategic Trade Control 9 (2024); Tal Mimran & Lior Weinstein, *The Need for Oversight on Surveillance Technologies: A (Painful) Perspective from Israel*, Forthcoming, CCDCOE (2024). [↑](#footnote-ref-275)
275. Maria Shagina, The Role of Export Controls in Managing Emerging Technology, in The Implications of Emerging Technologies in the Euro-Atlantic Space 59–60 (Jan Berghofer et al. eds., Palgrave Macmillan 2023), <https://doi.org/10.1007/978-3-031-24673-9_4>; Olga Torres & Derrick Kyle, Persistent Errors in the Export Classification of Software Products (Apr. 20, 2024), available at <https://www.torrestradelaw.com/posts/Persistent-Errors-in-the-Export-Classification-of-Software-Products/352>. [↑](#footnote-ref-276)
276. Fidler, *supra note* 228. [↑](#footnote-ref-277)
277. Bruce Berkowitz, *Keeping Secrets in the Digital Age*, Hoover Dig. 106 (2001). [↑](#footnote-ref-278)
278. Stowsky, *supra note* 29, 23-24. [↑](#footnote-ref-279)
279. Shagina, *supra note* 275, at 60. [↑](#footnote-ref-280)
280. Coveri 2025, supra note 6, at 82. [↑](#footnote-ref-281)
281. Coveri 2024, supra note 6, at 88; Farrell & Newman, supra note 110. [↑](#footnote-ref-282)
282. Huq, *supra note* 69, at 41-42. [↑](#footnote-ref-283)