The Militarization of Technology:

The Weaponization of Emerging Technologies and Its Impact on Human Rights in Indonesia



The Militarization of Technology: The Weaponization of Emerging Technologies and Its Impact on Human Rights in Indonesia

2026

The Militarization of Technology: The Weaponization of Emerging Technologies and Its Impact on Human Rights in Indonesia

Authors
Adzkar Ahsinin
Ikhsan Yosarie
Nurul Izmi
Kezia Khatwani
Octania Wynn
Naira A. Wibisono

Editor
Sueb

Translator
Indra Krishnamurti

Layout Designer
Dodi Sanjaya

Illustrator
Amry Al Mursaalat

Publisher
Institute for Policy Research and Advocacy (ELSAM) 2026
Jl. Siaga II No. 31, Pejaten Barat, Pasar Minggu, Jakarta 12510



TABLE OF CONTENTS

CHAPTER I INTRODUCTION 1

1. Background 1
2. Problem Formulation 3
3. Research Methods 3

CHAPTER II DUAL-USE TECHNOLOGY, THE MILITARY-INDUSTRIAL COMPLEX, AND HUMAN RIGHTS 5

1. Dual-Use Technology 5
2. Military-Industrial Complex in the Indonesian Context 17
3. What is the Human Rights Impact of the Military's Use of Surveillance Technology? 17
4. What are the Regulations and Accountability Regarding the Militarization of Technology? 36
5. The Use of Dual-use Technology in the Context of Indonesian Military Modernization and Its Impact on Human Rights 49
6. Dual-use Technology in the Context of the Military-Industrial Digital Complex: The Increasingly Blurred Civilian-Military Demarcation 56
7. The Intersection of the Rise of Militarization and the Use of Dual-use Technology: Identifying Its Impact on Human Rights 83

CHAPTER III CONCLUSION AND RECOMMENDATIONS 103

Conclusion 103

Recommendations 103

BIBLIOGRAPHY 105

PROFILE 119

“The biggest danger is the fear in our heads. The fear that the existing system imposes on us. This fear is the biggest obstacle in the struggle.”

Munir Said Thalib (1965-2004), Human Rights Activist

CHAPTER I
INTRODUCTION

1. Background

American president Dwight D. Eisenhower had warned of the dangers of the military-industrial complex in his farewell address on January 17, 1961. The warning was delivered in the context of the increasingly close ties between the military, the arms industry and the government. Eisenhower feared the undue influence of this combination on government decision-making, potentially endangering freedoms and democratic processes.[1]

Eisenhower's warning becomes increasingly relevant as technology companies are increasingly more involved in the defense sector. As technology advances, the configuration of the military-industrial complex is changing. While previously the conventional arms industry was the primary actor in the defense ecosystem, the development of digital technology has brought Big Tech companies with immense economic and technological power to the arena. This power stems from their control of knowledge, research and development, and the digital infrastructure and cutting-edge technologies, such as artificial intelligence and cloud computing, needed in both the civilian and military sectors. Big Tech's involvement in the defense sector is no longer limited to the provision of technology but also reflects a shift in the center of power within the military-industrial complex. This change has given rise to a phenomenon known as the *digital-military-industrial complex*, characterized by the growing role and influence of technology companies within the defense ecosystem.[2]

The changing configuration of the military-industrial complex is also related to the development of the militarization of technology, which is characterized by the increasingly widespread use of technology for military purposes. Furthermore, the militarization of technology is also reflected in the expanding influence of the military in the realm of technology and civilian life. This influence is realized through the involvement of military actors, the expansion of military roles and practices, and the adoption of military perspectives in the development, procurement, and use of technology. This trend is evident in the following four phenomena.[3]

First, the use of data-driven systems for military purposes. Surveillance technology, data analytics, and artificial intelligence are increasingly being used in military operations, including to monitor activity, identify individuals, and determine targets. In Israel, for example, the military uses the Lavender artificial intelligence system to analyze mass surveillance data and identify individuals suspected of being Hamas members. The use of this system has reportedly contributed to misidentification and civilian casualties.

Second, the involvement of technology companies in the defense sector. Big Tech companies and startups, which initially focused on developing technology and infrastructure for commercial and civilian needs, are increasingly entering the defense sector. This involvement is evident, among other things, in the provision of technology originally developed for the civilian market but also used for military purposes as dual-use technology.

---

[1] James Ledbetter, *Unwarranted Influence: Dwight D. Eisenhower and the Military-Industrial Complex* (New Haven, CT: Yale University Press, 2011).

[2] Andrea Coveri, Claudio Cozza, and Dario Guarascio, "Big Tech and the US Digital-Military-Industrial Complex," *Intereconomics* 60, no. 2 (2025): 81–87, https://doi.org/10.2478/ie-2025-0017.

[3] Privacy International, "What Is Militarization of Tech?" https://privacyinternational.org/long-read/5668/what-militarization-tech.

Third, the shift of defense technology to the civilian sector. Technology used in conflict is increasingly being diverted to law enforcement and public services. One example is Palantir, which provides data analytics technology for military needs, migrant surveillance, predictive policing, and even healthcare.

Fourth, the adaptation of conflict technology for commercial purposes. Technologies used in conflict are also adapted for commercial purposes, such as the use of facial recognition technology for surveillance in the Palestinian territories for civilian purposes, such as schools and hospitals. Conversely, commercial technologies, such as satellite imagery, are also used for military purposes.

These four phenomena demonstrate the increasingly blurred boundaries between the military and civilian spheres, both in the development and use of technology and in the roles of the actors involved. This becomes problematic when technology and the involvement of military actors expand into the civilian sphere, thereby expanding military practices and perspectives in public life. Without adequate legal boundaries, transparency, accountability, and oversight mechanisms, these developments can increase the risk of human rights violations, including the rights to privacy and freedom of expression.

In the Indonesian context, the involvement of technology companies in the security sector is evident, among other things, through the collaboration between Huawei and the National Cyber and Crypto Agency (BSSN) in the field of cybersecurity. Since 2019, the two parties have implemented various programs, including seminars, joint university activities, and certification programs. In 2023, they renewed their memorandum of understanding, which includes expanding cooperation, facilitating further learning, and providing professional certification in the field of cybersecurity.[4] This development demonstrates the involvement of foreign technology companies in building the Indonesian government's digital security capacity.

From the defense side, budget increases are also part of this development. During the administration of President Prabowo Subianto, the defense budget increased from Rp135 trillion to Rp165.2 trillion.[5] This budget increase requires further examination of its spending composition, particularly allocations for technology procurement and surveillance systems, to identify the extent to which the increase in defense spending is related to the development of the defense technology ecosystem.

The expansion of the military's role in the digital realm is also an issue that requires careful attention. Amendments to the Indonesian National Armed Forces Law (TNI) broaden the scope of military operations other than war (MOOTW) duties, including assistance in addressing cyber defense threats.[6] This expansion of duties raises questions about the limits of the military's authority in the digital space, particularly when it intersects with law enforcement and oversight of public activity. A TNI official's statement regarding alleged criminal activity in Ferry Irwandi's post following the August 2025 demonstration is one example that needs to be examined within the context of the limits of military involvement.[7]

---

[4] Indonesia Computer Security Incident Response Team Community, "Huawei dan BSSN Kerja Sama, Perkuat Keamanan Ruang Siber Nasional," https://csirt.or.id/berita/perkuat-keamanan-ruang-siber-huawei-kerjasama-bssn, accessed August 20, 2026.

[5] Kurnia Rahayu, "Sejalan dengan Visi Prabowo, Anggaran Pertahanan Naik Jadi Rp 165 Triliun," *Kompas.id*, September 3, 2024, https://www.kompas.id/artikel/sejalan-dengan-visi-prabowo-anggaran-pertahanan-naik-jadi-rp-165-triliun.

[6] See Law Number 3 of 2025.

[7] detikNews, "Dansat Siber TNI sebut Ada Dugaan Pidana Ferry Irwandi, Konsul ke Polda Metro", https://www.detik.com/sumut/berita/d-8102444/dansat-siber-tni-sebut-ada-dugaan-pidana-ferry-irwandi-konsul-ke-polda-metro, accessed August 21, 2026.

Furthermore, discussions on the Cybersecurity and Resilience Bill (RUU KKS) have also raised questions about the division of authority for cybersecurity and defense, as well as the protection of public rights in the digital space. This situation creates a conducive ecosystem for the militarization of technology, given the bill's state-oriented approach, instead of oriented towards individual security and citizen protection.

These developments demonstrate several aspects of the militarization of technology in Indonesia, ranging from the involvement of technology companies in the security sector, increased defense spending, to the expansion of the military's role in the digital realm. These developments raise questions regarding the limits of military authority, governance and accountability for technology development, procurement, and use, and their implications for human rights. The use of technology, particularly dual-use technology, needs to be examined not only in terms of its use for military purposes, but also in terms of how it can extend military influence and practices into the civilian sphere.

Based on this, the Institute for Policy Research and Advocacy (ELSAM) initiated research on the militarization of technology in Indonesia. This research aims to map the technology militarization ecosystem, including the actors involved, the types of technology, and the relationships and mechanisms for procurement. This research also examines the regulations and accountability mechanisms for the development, procurement, and use of technology, as well as their implications for human rights. Specifically, this research examines efforts to ensure that military use of technology remains in accordance with the principles of human rights protection and identifies challenges and opportunities in redress mechanisms for victims.

2. Problem Formulation

Based on the background above, this study asks the following research questions:

1. What is the state of the militarization of technology ecosystem in Indonesia?
2. What is the legal framework and oversight and accountability mechanisms for the development, procurement, and use of technology in the context of the militarization of technology in Indonesia?
3. What is the impact of the militarization of technology, particularly the use of dual-use technology, on human rights?
4. How to ensure that the development, procurement and use of technology does not expand military practices and influence that are contrary to the principle of protecting human rights?
5. What are the challenges and opportunities in the redress mechanism for victims of human rights violations related to the militarization of technology?

3. Research Methods

This research uses the socio-legal research approach. This approach views law not only as a set of written rules, but also in relation to the social and institutional contexts and their practical application. This approach is used to analyze the development of the militarization of technology in Indonesia by examining the relationship between policies, institutions, and practices of technology development, procurement, and use. The analysis includes the actors involved, the allocation of state resources, and the purposes and contexts of technology use.

The research data was obtained through document studies using various sources. These sources include laws and regulations, policy and institutional documents, research reports, academic publications, media coverage, and other open sources.

CHAPTER II
DUAL-USE TECHNOLOGY, THE MILITARY-INDUSTRIAL COMPLEX, AND HUMAN RIGHTS

1. Dual-Use Technology

Dual-use technology refers to technology that can be used for both civilian and military purposes. This concept also encompasses knowledge and technology that can be used for both beneficial and harmful purposes, including those with the potential to cause large-scale harm, whether through weapons development or without the weaponization process.[8] Thus, dual-use technology relates not only to the possibility of using a technology for different purposes, but also to the potential impacts that arise from its use.

Initially, the term dual-use technology was often associated with nuclear materials that could be used to generate energy or develop weapons. As technology advanced, its scope has expanded to include artificial intelligence, cybertechnology, biotechnology, and advanced materials. This expansion also relates to the increasingly close relationship between the civilian technology industry and the defense sector. Companies developing technology for the commercial market can simultaneously meet the needs of both the government and the military. In this context, dual-use technology can be understood not only as a technological characteristic, but also as a product development and market expansion strategy.[9]

One conceptual issue in understanding dual-use technology is the broad scope of the term. Not all technologies used for both civilian and military purposes are necessarily dual-use technologies in the weaponry sense. The internet, power grids, cameras, and communication systems, for example, can be utilized by both civilians and the military, but their use by the military does not automatically make them weapons. Therefore, it is necessary to distinguish between technology that has multiple functions, and technology that has the potential to be used to develop weapons or cause large-scale harm.[10]

This issue is becoming increasingly complex with the increasing interconnectedness between the development and use of technology in the civilian and military spheres. Technology developed for civilian needs can be utilized in the defense sector, while technology developed for military purposes can also be used in civilian activities. This interconnectedness presents challenges in identifying potential risks and determining the responsibilities of technology developers, suppliers, and users, particularly when its use has detrimental impacts.

In relation to human rights and democracy, the use of dual-use technology has the potential to pose risks when not accompanied by limitations on authority, transparency, and adequate oversight mechanisms. These risks include human rights violations, the expansion of surveillance practices into the population, and restrictions on civil liberties that could undermine democratic oversight. In armed conflict, the use of technology must also comply with the principle of distinction in international humanitarian law, which requires parties to a conflict to distinguish between civilians and combatants, as well as civilian objects and military targets.[11]

---

[8] Miller, *Dual Use Science and Technology*.
[9] MIT Mission Innovation
[10] Miller, *Dual Use Science and Technology*.
[11] International Committee of the Red Cross (ICRC), "Methods and Means of Warfare," https://www.icrc.org/en/law-and-policy/methods-and-means-warfare.

1.1. Types of Dual-use Technology

1.1.1. Artificial Intelligence

Artificial Intelligence (AI) is one of the most prominent examples of the dual-use nature of technology in contemporary technological development. The development of AI is inextricably linked to the history of computing, warfare, and the need for states to process information more quickly. While AI is currently often understood through civilian applications such as search engines, chatbots, recommendation systems, autonomous vehicles, or data analysis, some of its technological foundations have a long history of ties to defense interests. This connection can even be traced back to the time of Alan Turing and World War II.

Alan Turing was a key figure in the development of modern computer science. During World War II, Turing worked at Bletchley Park, the British codebreaking center, and was involved in efforts to decipher German communications encrypted using the Enigma machine. Turing developed electromechanical devices and methods that helped accelerate the search for Enigma configurations, allowing the Allies to analyze German military messages. However, this work could not yet be called artificial intelligence in the modern sense. Its significance lies in the idea that reasoning and search processes previously performed by humans could be formalized and systematically performed by machines.[12]

After the war ended, Turing began to develop more fundamental questions about the capabilities of machines. In his famous article, "Computing Machinery and Intelligence," published in 1950, Turing posed the question: "Can machines think?" Rather than attempting to define abstractly what "thinking" meant, he proposed what became known as the Imitation Game or Turing Test, a way to assess whether a machine's communication behavior could resemble that of a human. Turing also discussed the possibility of learning machines, machines that could not only execute fixed instructions but also undergo a learning process.[13]

Turing's thinking became one of the intellectual foundations for the birth of AI as a scientific discipline. However, the term artificial intelligence itself was not introduced until several years later. In 1955, John McCarthy, along with Marvin Minsky, Nathaniel Rochester, and Claude Shannon, proposed organizing the Dartmouth Summer Research Project on Artificial Intelligence. The meeting, held in the summer of 1956, became known as one of the milestones in the birth of AI as a distinct field of research. The researchers started from the assumption that various aspects of human learning and intelligence could, in principle, be described precisely enough to allow machines to simulate them.[14]

Since its inception, AI research has also had a close relationship with defense institutions. During the Cold War, the United States viewed computing and automation technologies as part of strategic competition. Through the Defense Advanced Research Projects Agency (DARPA), the US government subsequently funded research into human-computer interaction, robotics, pattern recognition, information processing, and machine intelligence. DARPA states that its institutional investment in AI can be traced back to the 1960s, including research into symbiotic relationships between humans and machines.[15] In the 1980s, the relationship between AI and military interests became increasingly explicit through the Strategic Computing Initiative, which

---

[12] Central Intelligence Agency (CIA), "The Enigma of Alan Turing," April 10, 2015, https://www.cia.gov/stories/story/the-enigma-of-alan-turing/.

[13] Sam J. Tangredi and George Galdorisi, eds., *AI at War: How Big Data, Artificial Intelligence, and Machine Learning Are Changing Naval Warfare* (Annapolis, MD: Naval Institute Press, 2021), 51.

[14] Tangredi and Galdorisi, eds., *AI at War*, 52.

[15] Defense Advanced Research Projects Agency (DARPA), "AI Next," https://www.darpa.mil/research/programs/ai-next. DARPA traces the history of its AI program to J.C.R. Licklider's 1960s research on the relationship between human and machine intelligence.

sought to develop intelligent computing systems for various defense needs. Programs during this period began to envision autonomous ground vehicles, pilot assistance systems, and battle management systems. This means that from the very beginning of AI development, military interests were not simply directed at creating machines that could "think," but at more operational questions: how machines could help the military perceive the environment, process information, plan actions, and accelerate decision-making.

One significant operational use of AI occurred during the 1990–1991 Gulf War, when the United States military used the Dynamic Analysis and Replanning Tool (DART) to assist in logistics planning and the movement of personnel and equipment. DART used automated planning and scheduling techniques to address highly complex military transportation issues. According to DARPA records, the system enabled deployment plans that previously took days to complete in a matter of hours.[16] This example is important because it demonstrates that the use of AI in warfare does not always begin with weapons delivery systems. Rather, AI first gains military value because of its ability to process complexity. AI can be used to process intelligence information, support operational planning and decision-making, and optimize logistics management and resource scheduling.[17]

More fundamental changes have occurred since the late 2000s and especially throughout the 2010s through the development of machine learning, deep learning, big data, cloud computing, increased semiconductor capacity, and the availability of vast amounts of digital data. Unlike many Cold War-era AI programs that relied heavily on government funding, contemporary AI advances are rapidly evolving through the commercial technology industry. Technology companies are developing computer vision, speech recognition, data analytics, cloud services, navigation systems, and generative AI for the civilian market. However, these technologies are dual-use in nature, as they can be relatively quickly adapted for security and defense purposes. Consequently, innovation patterns are beginning to shift. Whereas in the past technology shifted from military research to civilian applications, in the digital age the reverse is true. Technology begins as commercial innovation and is then adopted by the military. This shift explains why technology companies, cloud providers, chip manufacturers, AI companies, and defense-tech startups are increasingly becoming part of the defense ecosystem, even though their underlying products are not always developed as weapons. Privacy International and PAX even described this process in 2026 as a convergence between the technology and arms industries, leading to a new form of military-industrial complex.[18]

A key milestone in what would become known as algorithmic warfare was the creation of Project Maven by the United States Department of Defense in April 2017. The program was formally established as the Algorithmic Warfare Cross-Functional Team to accelerate the integration of big data, AI, and machine learning into defense operations. In its early stages, Project Maven was aimed at addressing a very concrete problem: the military had volumes of footage and imagery from intelligence, surveillance, and reconnaissance (ISR) systems that were too large for humans to analyze manually. Computer vision algorithms were then used to help detect and classify objects in the imagery and video, allowing analysts to transform the vast amounts of data into usable information for operations. The Department of Defense described its goal as transforming vast volumes of data into actionable intelligence. This shift was significant because algorithms began to intersect between sensors and human decisions: technology was no longer simply

[16] DARPA, "Breakthrough Technologies for National Security," 2015. DART was used in Operations Desert Shield and Desert Storm to accelerate military logistics and deployment planning.

[17] Emelia Probasco, Helen Toner, Matthew Burtell, and Tim GJ Rudner, "AI for Military Decision-Making: Harnessing the Advantages and Avoiding the Risks," *Center for Security and Emerging Technology*, April 2025, https://doi.org/10.51593/20240028.

[18] Privacy International and PAX, *Tech Giants, the Arms Industry and the Weaponization of AI: When Algorithms Go to War*, June 2026.

gathering information, but helping to determine what information was considered relevant, what objects to pay attention to, and which threats to prioritize.

In this sense, algorithmic warfare can be understood as a form of warfare in which algorithms are increasingly used to process information, recognize patterns, classify objects, generate predictions or recommendations, and accelerate decision-making in military operations. AI can be present in almost the entire operational chain: data collection through sensors; satellite or drone image processing; object recognition; potential threat identification; prioritization; action recommendations to commanders; and integration with weapons systems. The development of Project Maven demonstrates how this function is increasingly integrated into the targeting process. A 2022 Government Accountability Office (GAO) report, for example, noted the development of target recognition capabilities through Scarlet Dragon, which uses Project Maven data. In a live-fire demonstration in October 2021, these AI capabilities were used across the Army, Air Force, and Navy to help identify targets that are then attacked.[19] Thus, the important issue in algorithmic warfare is not merely whether AI automatically "decides to kill," but how AI is increasingly integrated into the process of finding, identifying, tracking, targeting, engaging, and assessing, which previously relied heavily on human judgment.

However, AI does not necessarily mean autonomous weapons. Not all autonomous weapons systems use AI, and not all military uses of AI are weapons systems. The ICRC distinguishes several key applications of AI in armed conflict: the use of AI to enhance autonomy in robotic systems, including weapons; the use of AI in cyber and information operations; and the use of AI as a decision-support system.[20] AI can also be used for logistics, predictive maintenance, navigation, intelligence, surveillance, or information management without directly attacking targets. However, the closer AI is placed to the decisions that determine who or what is targeted, the more serious questions about human control, reliability, bias, transparency, and accountability become. The United States government, through DoD Directive 3000.09, requires that autonomous and semi-autonomous weapons systems be designed to allow commanders and operators to exercise an appropriate level of human judgment regarding the use of force. The ICRC also emphasizes the importance of maintaining human judgment, particularly when AI systems are used in decisions that have serious consequences for human life.

The dual-use nature of AI ultimately makes algorithmic warfare have consequences that extend beyond the battlefield. Facial recognition, behavioral analysis, geolocation, database fusion, computer vision, and biometric processing technologies can move between military, security, border, policing, and domestic surveillance contexts. The ICRC warns that the use of AI could enable the fusion of data from sensors, communications, databases, social media, and biometric data to produce algorithmic assessments of individuals, including their status or potential actions. Privacy International also highlights that data-driven technologies used in warfare can simultaneously support mass surveillance and the expansion of the surveillance state.[21] This means that AI as a dual-use technology not only blurs the boundaries between civilian and military technology at the product level, but also the lines between the battlefield and civilian space. Therefore, analysis of the militarization of AI needs to consider not only the technology used and the capabilities it generates, but also the companies that develop it, the data used to train and run the system, the digital infrastructure that supports it, the procurement

[19] US Department of Defense, "Project Maven to Deploy Computer Algorithms to War Zone by Year's End," July 21, 2017; and "Project Maven Industry Day Pursues Artificial Intelligence for DoD Challenges," November 3, 2017.
[20] International Committee of the Red Cross (ICRC), *Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach,* June 2019.
[21] International Committee of the Red Cross (ICRC), "FAQ: Artificial Intelligence (AI) in the Military Domain," June 11, 2026, https://www.icrc.org/en/article/faq-artificial-intelligence-in-military-domain; Privacy International and PAX, *Tech Giants, the Arms Industry and the Weaponization of AI: When Algorithms Go to War*.

mechanisms, and the extent to which algorithm-based decisions remain legally and democratically accountable.

1.1.2. Unmanned Aerial Vehicles (UAVs)

Unmanned Aerial Vehicles (UAVs), or drones, are a technology widely used by militaries and non-state armed groups in conflict zones. However, drones also have dual-use characteristics, as they can be used for various civilian purposes, including by multinational corporations, humanitarian organizations, and emergency response teams for mapping, disaster monitoring, aid distribution, and various other needs that support public interests.

On the other hand, drones are also used for intelligence, surveillance, and documenting human rights violations. In a military context, drones can be used to monitor individuals or groups deemed to have a strategic profile or importance. Data collected through this surveillance can then be processed and entered into target lists, either compiled by humans or with the help of algorithmic systems. These lists can then be used to determine the location or target of attack operations using Medium Altitude Long Endurance (MALE) drones or smaller loitering munition systems.[22]

These characteristics demonstrate that drones have a wide range of strategic functions. On the one hand, drones are a relatively flexible and accessible technology that offers numerous benefits to society. However, on the other hand, the same technology can be integrated into long-range weapons systems for surveillance, target identification, and even lethal strikes. Thus, drones are one of the clearest examples of how dual-use technology can move from civilian and humanitarian functions to surveillance, intelligence, and the use of force in a military context.

The use of drones in military operations raises ethical issues because it allows attacks to be carried out with much less risk to the militaries of user countries. UAVs are often viewed as a means of conducting more precise and efficient attacks. However, the ease of remote operation has also given rise to debates about the limits of the use of force, the legitimacy of targeting, and the protection of civilians.[23]

According to SIPRI findings released in April 2026, global military spending trends show a shift in both scale and geographic distribution. The global military burden increased from 2.4 percent of global GDP in 2020 to 2.5 percent in 2025, with average military spending reaching 6.9 percent of total government expenditure and approximately US$352 per capita. Interestingly, this increase in global spending persisted despite a decline in US military spending. Sharp spending growth in Europe and continued increases in Asia and Oceania offset this decline; in fact, if the United States were excluded, global military spending would increase by 9.2 percent in 2025.

This shift also indicates a growing portion of the budget being directed toward modern military technology and capacity. India, for example, increased its military spending by 8.9 percent to US$92.1 billion, particularly following the conflict with Pakistan in May 2025 involving fighter jets, drones, and missiles. Meanwhile, Iran significantly increased funding for its domestic industry producing military aircraft, drones, and ballistic missiles. These developments demonstrate that increased defense spending is not only related to budget size, but also to strengthening the defense industry and investing in technologies such as drones, aerial systems, and missiles. At the same time, the existence of off-budget financing mechanisms, such as those found in Iran's

[22] James Patton Rogers, "Introduction: Why Study Drones?" in *De Gruyter Handbook of Drone Warfare*, ed. James Patton Rogers (Berlin/Boston: De Gruyter, 2024), 2.
[23] Rogers, "Introduction: Why Study Drones?" 10.

drone and missile programs, also highlights the transparency challenges in fully measuring the scale of military spending.[24]

The Israeli Defense Forces' use of commercial drones in operations in Gaza demonstrates how technology originally developed for civilian purposes can undergo militarization and weaponization. DJI, a Chinese technology company known as one of the world's leading manufacturers of commercial drones, primarily develops its products for various civilian purposes, such as photography, mapping, agriculture, and inspection. However, drones manufactured by DJI have also been used by Israel for military purposes since at least before the 2023 Gaza war. A 2018 Bellingcat investigation found the use of a number of DJI commercial drones, including the Matrice 100 and Matrice 600, by Israel around Gaza. The DJI Matrice 600 was modified with a mechanism that allowed the release of multiple tear gas grenades against demonstrators during the Great March of Return.[25]

The use of commercial drones has grown since the outbreak of the Gaza genocide in October 2023. In April 2024, Israeli media outlet Globes reported that the Israel Defense Forces (IDF) ordered thousands of drones manufactured by DJI and Autel Robotics for close-range imaging and reconnaissance, including for gathering intelligence during operations in Gaza.[26] This development demonstrates that commercial drones can meet military operational needs without having to develop a dedicated UAV platform. Their relatively low cost, commercial availability, camera capabilities, and operational flexibility allow civilian drones to be quickly adapted for intelligence, surveillance, and reconnaissance (ISR) functions.

The function was then reportedly expanded from surveillance to more direct use in combat operations. An investigation by Al Jazeera's Sanad verification unit published in May 2025 found indications that several types of DJI drones had been modified by the Israeli military for various functions in operations in Gaza, including (1) DJI Mavic reportedly used for reconnaissance and target acquisition, (2) DJI Avata, a small drone primarily designed for video recording, used to navigate and map tunnel networks, (3) DJI Agras, a drone designed for agricultural purposes modified and used to drop explosives on a building belonging to the humanitarian organization IHH in Jabalia in July 2025 as well as its use in another attack in Beit Lahia.[27]

1.1.3. Surveillance and Biometric Technology.

Surveillance technology is not limited to facial recognition or biometric technology, but includes a variety of devices and systems that enable states and other actors to collect, access, intercept, identify, track, and analyze information about individuals, groups, communications, or a region. Surveillance technology is divided into network surveillance, which is surveillance carried out through telecommunications network infrastructure, and tactical surveillance, which allows direct access to a person's device remotely, such as IMSI Catchers and Intrusion Technologies.

Over time, this ecosystem has also encompassed spyware, geolocation systems, CCTV, facial recognition, social media monitoring, mobile phone extraction, drone surveillance, and AI-based analysis systems. In the defense context, surveillance has long been part of the intelligence

[24] Xiao Liang, Nan Tian, Diego Lopes da Silva, Lorenzo Scarazzato, Zubaida Karim, and Jade Guiberteau Ricard, "Trends in World Military Expenditure, 2025," *SIPRI Fact Sheet* (Stockholm International Peace Research Institute (SIPRI), April 2026), 1.

[25] Nick Waters, "First ISIS, then Iraq, now Israel: IDF Use of Commercial Drones," *Bellingcat*, June 18, 2018, https://www.bellingcat.com/news/middle-east/2018/06/18/first-isis-iraq-now-israel-idf-use-commercial-drones/, accessed September 3, 2026.

[26] Assaf Gilead, "IDF Procurement of Chinese Drones Raises Concerns," *Globes*, April 25, 2024. https://en.globes.co.il/en/article-idf-procurement-of-chinese-drones-raises-concerns-1001477502

[27] Al Jazeera, "Israel Retrofitting DJI Commercial Drones to Bomb and Surveil Gaza," May 8, 2025, https://www.aljazeera.com/news/2025/5/8/israel-retrofitting-dji-commercial-drones-to-bomb-and-surveil-gaza, accessed September 5, 2026.

function, particularly through the concept of intelligence, surveillance, and reconnaissance (ISR). However, digitalization has changed the scale and character of such surveillance. Surveillance is no longer simply conducted by observing an object or intercepting specific communications, but increasingly relies on the collection and integration of large amounts of data, including communication metadata, location, biometric data, social media activity, satellite and drone imagery, and data from various sensors. Privacy International describes data as a central element in the militarization of contemporary technology because data-driven systems enable states to detect behavioral patterns, map relationships between people, identify activities deemed deviant, and even help shape targets for security or military operations.[28] The process of militarization thus occurs not only when a camera or software is directly used on the battlefield, but also when the collected data is used for intelligence functions, threat identification, targeting, and security decision-making.

One of the most intrusive forms of surveillance is spyware, which works by covertly gaining access to a target's or victim's digital devices. For example, Pegasus, developed by the NSO Group, can access messages, emails, contacts, calls, microphones, cameras, and various other data on a victim's device in real time. ELSAM's research, titled "Privacy in a Glass House: Challenging Spyware Accountability in Indonesia," found that military institutions have spent at least Rp1.3 trillion on surveillance technology, with unclear procurement processes and intended uses. Investigations by Amnesty International and Citizen Lab have documented the majority of Pegasus usage targeting journalists, human rights defenders, activists, and civil society actors in various countries. In Palestine, for example, an independently reviewed forensic analysis by Amnesty International and Citizen Lab confirmed that six devices belonging to Palestinian human rights defenders had been infected by Pegasus in 2020–2021.[29] These cases demonstrate how technology marketed for the purposes of combating terrorism or searching for wanted suspects has the potential to be used against parties unrelated to security threats.

Besides spyware, surveillance can also be conducted without directly hacking the target device. Lawful interception systems, for example, allow authorities to obtain communications through telecommunications operator infrastructure, while IMSI catchers work by masquerading as cellular towers so that nearby devices connect and reveal their network identity and location information. Some types of IMSI catchers can also intercept communications, so their use at demonstrations or political gatherings can collect data not only from the targeted individual but also from others around them.[30] In addition to spyware and IMSI catchers, there are several other surveillance technologies such as (1) facial recognition that can be used to identify someone from public cameras, (2) social media monitoring that can map activities, friendship networks, or political views, (3) location data that can show movements, (4) mobile phone extraction that can obtain data from confiscated phones. This information can then be combined with databases and analyzed through AI systems to form profiles, watchlists, or risk assessments of certain individuals.

2. Military-Industrial Complex in the Indonesian Context

The concept of the military-industrial complex (MIC) is essentially used to explain the structural relationship between military institutions, government, and industry that derive economic interests from the development and maintenance of defense forces. Therefore, the MIC should

[28] Privacy International, "What Is Militarization of Tech?" 2025, https://privacyinternational.org/long-read/5668/what-militarisation-tech, accessed September 7, 2026.
[29] Amnesty International Security Lab and Citizen Lab, "Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware," 8 November 2021. https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/ accessed 7 September 2026.
[30] Privacy International and ELSAM Team, *Privasi 101: Panduan Memahami Privasi, Perlindungan Data, dan Surveilans Komunikasi* (Jakarta: ELSAM and Privacy International, 2015), 46.

not be understood narrowly as simply "cooperation between the military and arms companies." The concept refers to an ecosystem of interests in which security needs generate budgets, research, procurement, and contracts; industry derives markets from these needs; and industrial capacity and technological developments can, in turn, influence how a country defines its defense needs. Even before the term MIC was introduced by Eisenhower, C. Wright Mills in The Power Elite (1956) had identified the increasing interconnectedness of political elites, large corporations, and the military in the United States. According to Mills, the development of these major institutions produces a power structure in which economic, political and military decisions are increasingly difficult to separate from one another.[31]

The development of the MIC is inextricably linked to the transformation of warfare during World War II and the Cold War. World War II mobilized not only armies but also companies, universities, scientists, laboratories, and industrial production capacity to produce aircraft, radar, communications, rockets, computers, and even nuclear weapons. These structures were not completely dismantled after the war's end. Thomas C. Lassman points out that in 1946, while still Chief of Staff of the United States Army, Eisenhower established a research and development division within the War Department to accelerate weapons innovation and maintain military technological superiority. The Cold War then made the state's relationship with the military and industry more permanent, as competition with the Soviet Union necessitated continued defense spending, technological research, and weapons production. Thus, a long-term relationship was formed between military demand, public funding, technological research, and industrial production.[32]

According to Eisenhower, the intersection of the vast military and the arms industry created new economic and political forces that had the potential to exert unwarranted influence over government processes. What is often overlooked is that Eisenhower also linked these changes to the technological revolution, in which research became increasingly expensive, complex, and dependent on government funding and direction.

In the 21st century, the development of digital technology has transformed the character of contemporary defense and security. Military capability is no longer solely determined by the possession of conventional weaponry such as rifles, tanks, warships, and fighter jets, but increasingly relies on artificial intelligence, surveillance systems, unmanned aerial vehicles (UAVs), satellites, data processing, and so on. This change has also blurred the boundaries between civilian and military technology, as some of these technologies are dual-use, developed or used for civilian purposes but can be adapted for defense, intelligence, and military operations. Similar changes can be observed in the development of Indonesian defense policy. The Defense Industry Policy Committee (KKIP), for example, has designated ten key technologies as a priority program of the defense industry, including unmanned aerial vehicles and military satellites. At the same time, the Ministry of Defense and the Indonesian National Armed Forces (TNI) are beginning to place significant emphasis on AI, cyber defense, unmanned systems, and the integration of various sensor platforms.[33]

These developments demonstrate that the militarization of technology needs to be viewed as an ecosystem, not simply a process of procuring primary weapons systems. This ecosystem consists of at least four interrelated elements: technology, military and state institutions, the defense industry and private companies, and budget and procurement mechanisms. Deikin

[31] C. Wright Mills, *The Power Elite* (New York: Oxford University Press, 1956), 275.
[32] Thomas C. Lassman, "Putting the Military Back into the History of the Military-Industrial Complex: The Management of Technological Innovation in the US Army, 1945–1960," *Isis* 106, no. 1 (2015): 94–120, https://doi.org/10.1086/681038.
[33] Defense Industry Policy Committee (KKIP), "Rencana Aksi Industri Pertahanan: Penguasaan Sepuluh Teknologi Prioritas," February 20, 2023, https://www.kkip.go.id/2023/02/20/rencana-aksi-industri-pertahanan-penguasaan-sepuluh-teknologi-prioritas/.

demonstrates that weapons production is not solely driven by defense needs, but also by the economic interests of actors who benefit from continued weapons production and procurement. Within the framework of the military-industrial complex, these interests can form a mutually reinforcing relationship: threat perceptions drive budget increases and procurement; procurement creates a market for industry; while the existence of established industrial capacity and economic interests can contribute to continued demand for defense technology. Therefore, the military-industrial complex cannot be understood as merely a contractual relationship between the military and companies, but rather as an ecosystem in which security interests, state policy, public budgets, industry, and technological development are intertwined.[34]

Moreover, this is also supported by a surge in defense budgets worldwide. According to the Stockholm International Peace Research Institute (SIPRI), global military spending in 2024 reached US$2.7 trillion, a 9.4% increase from the previous year, the highest annual increase since the end of the Cold War.[35] One of the countries experiencing this surge is Indonesia. On June 10, 2026, Defense Minister Sjafrie Sjamsoeddin conveyed to Commission I of the Indonesian House of Representatives that the ideal defense budget requirement for 2027 reaches Rp667 trillion, far exceeding the indicative ceiling set by the Ministry of Finance and Bappenas of Rp139 trillion. The Ministry of Defense then proposed an additional budget of Rp195 trillion, bringing the total actual proposal to the DPR to Rp334 trillion to support the modernization of weapons systems and the development of defense forces.[36]

One of the key characteristics of the militarization of contemporary technology is the increasingly blurred distinction between civilian and military technology. This phenomenon can be explained through the concept of dual-use technology. Drones are the most obvious example. They can be used for mapping, agriculture, disaster monitoring, photography, and delivery. However, similar platforms and technologies can be used for reconnaissance, surveillance, target acquisition, ammunition delivery, and even attack. The Ministry of Defense itself recognizes the dual-use nature of drones and their role as a technology transforming modern warfare.[37] AI magnifies this issue. Computer vision algorithms, for example, can be used to recognize objects in commercial applications, but can also be integrated into surveillance systems to identify people, vehicles, or targets. Cloud infrastructure used by companies and government agencies can also be used for the storage and processing of defense data. Satellite communication systems can serve both civilian communications and military operations.

These developments are already evident in Indonesia's defense orientation, but the MIC concept needs to be used with caution because the structure of Indonesia's defense industry differs from that of the United States. While the classic American MIC is largely supported by private defense companies, in Indonesia's case, the Indonesian defense industry has historically featured a far more dominant role among the state, state-owned enterprises, and private companies. The industry's roots can even be traced back to the colonial era: PT Pindad traces its roots back to the Constructie Winkel, founded in 1808; PT PAL traces its roots back to the Marine Etablissement in 1939; and the history of the aviation industry, which later evolved into PT Dirgantara Indonesia, can be traced back to the Dutch East Indies aviation facilities in the early 20th century.[38] In the

[34] Alexander Deikin, *An Alliance of the Monopolies and the Military: On the US Military-Industrial Complex* (Moscow: Novosti Press Agency, 1973), 20.

[35] Stockholm International Peace Research Institute (SIPRI), "Unprecedented Rise in Global Military Expenditure as European and Middle East Spending Surges," Press Release, April 28, 2025, https://www.sipri.org/media/press-release/2025/unprecedented-rise-global-military-expenditure-european-and-middle-east-spending-surges.

[36] Tempo, "Menhan: Kebutuhan Anggaran Pertahanan Tahun 2027 Rp 667 Triliun," https://www.tempo.co/politik/menhan-kebutuhan-anggaran-pertahanan-tahun-2027-rp-667-triliun-2266159, accessed July 3, 2026.

[37] Gede Priana Dwipratama, "Swarm Drone: Tantangan, Peluang dan Ancaman bagi Indonesia," Directorate General of Defense Potential, Ministry of Defense of the Republic of Indonesia, April 25, 2024, https://www.kemhan.go.id/pothan/2024/04/25/swarm-drone-tantangan-peluang-dan-ancaman-bagi-indonesia.html.

[38] Defense Industry Policy Committee (KKIP), "Sejarah Industri Pertahanan Nasional," https://www.kkip.go.id/sejarah.

independence era, these companies underwent nationalization and reorganization, becoming part of the country's strategic industries. As it developed, the orientation of Indonesia's defense industry was not only directed at meeting the needs of the Indonesian National Armed Forces (TNI) and the Indonesian National Police (Polri), but also at entering the international defense market. PT Pindad, for example, produces weapons, ammunition, and special vehicles for national defense needs as well as to generate revenue from other countries.

The company officially lists Myanmar as one of the countries to which it has exported its products, along with Malaysia, Brunei Darussalam, Timor-Leste, Singapore, Bangladesh, Laos, Thailand, South Korea, and the United States.[39] However, the presence of Myanmar on the list of export destinations does not in itself indicate that the products were sold to the junta after the February 2021 coup. DEFEND ID stated that PT Pindad's exports to Myanmar were made in 2016 in the form of sporting-specification ammunition for the ASEAN Armies Rifle Meet (AARM), and denied that PT Pindad's defense products were exported to Myanmar after the 2021 coup.

The issue of accountability then emerged in October 2023 when the Chinese Human Rights Organization (CHRO), the Myanmar Accountability Project (MAP), and former Indonesian Attorney General Marzuki Darusman filed a complaint with the National Commission on Human Rights (Komnas HAM) regarding the alleged sale of defense products by PT Pindad, PT PAL, and PT Dirgantara Indonesia to the Myanmar military.[40] The complainants alleged the promotion and alleged transfer of rifles, pistols, ammunition, combat vehicles, and other military equipment over a period of approximately a decade, including possible transactions after the February 2021 coup. Komnas HAM confirmed receipt of the complaint and stated that it would conduct a review to determine whether or not there were any alleged human rights violations, while also considering the issue of jurisdiction because the case involved parties outside Indonesia.

In addition to exports, dual-use technology is also increasingly being used in Indonesia. In 2024, the Indonesian Air Force stated that it would be using AI in air defense training and plans to expand the development of AI and cyber technology. The "Cakra" National Air Defense System is even designed to integrate sensors, shooters, and command and control (C2), with AI used to accelerate the decision-making process. This architecture includes integrated air defense, electromagnetic warfare, cyber and space, as well as the integration of sea, air, and land platforms. The development of the "Elang Hitam" MALE PTTA also illustrates this trend.[41] This program involves a consortium consisting of, among others, the Ministry of Defense, the Indonesian Air Force, PT Dirgantara Indonesia, PT LEN, as well as research institutions and universities, with an orientation towards integrating UAVs with weapons systems and C4ISR.

In security operations in Papua, the Indonesian National Armed Forces (TNI) has used drones primarily for surveillance, reconnaissance, and initial sweeps of operational areas, citing the need to reduce the risk to personnel. TNI Commander General Agus Subiyanto stated in December 2023 that drones are used to monitor routes and conditions before troops move into areas deemed vulnerable. In 2024, the Marine Corps also deployed the DJI Enterprise Matrice 350 RTK and DJI Enterprise Matrice 30 Series to support the Indonesian-Papua New Guinea Mobile Border Security Task Force; both drones are products of Chinese technology company DJI

[39] PT Pindad (Persero), "Kendarai Ranops Maung, Presiden Tinjau Divisi Munisi dan Apresiasi Kemampuan Lini Produksi PT Pindad," July 27, 2023, https://pindad.com/kendarai-ranops-maung-presiden-tinjau-divisi-munisi-dan-apresiasi- mampu-lini-produksi-pt-pindad.

[40] Chin Human Rights Organization (CHRO) and Myanmar Accountability Project (MAP), "Indonesian Arms Producers Accused of Illegal Sales to Myanmar," October 2, 2023, https://progressivevoicemyanmar.org/2023/10/02/press-release-indonesian-arms-producers-accused-of-illegal-sales-to-myanmar. The complaint names PT Pindad, PT PAL, and PT Dirgantara Indonesia and the alleged sale of various defense products to the Myanmar military.

[41] Defense Technology Agency, Ministry of Defense of the Republic of Indonesia, "Design Requirement Rancang Bangun Weapon Integration System PTTA MALE Konsorsium," July 7, 2025, https://www.kemhan.go.id/batekhan/2025/07/07/design-requirement-rancang-bangun-weapon-integration-system-ptta-male-konsortium.html.

and have been tested for their ability to continuously detect and track the movement of vehicles and personnel in the operational area. The M30 series can also be equipped with wide-angle, zoom, and thermal cameras, enabling surveillance and target identification in difficult terrain.[42]

Thus, the militarization of technology should not be understood as the creation of technologies that are initially exclusive to the military. Militarization also occurs when technology, expertise, data, and infrastructure with civilian functions are integrated into defense and security functions. This raises more complex governance issues. Regulations oriented toward "weapons" or "weapons systems" may be relatively easy to apply to rifles or tanks. However, the boundary becomes more difficult when the objects are algorithms, cloud computing, sensors, facial recognition, commercial drones, cyber tools, or data analysis software.

When viewed in a broader context, the development of the Indonesian defense industry is no longer limited to meeting domestic needs alone, but also to mastering technology, increasing production capacity and expanding international markets, including to the African region. One example is the relationship between PT Pindad and Rheinmetall Denel Munition (RDM), a defense industry company based in South Africa and a joint venture between Rheinmetall Waffe Munition of Germany and Denel of South Africa.[43] The collaboration between PT Pindad and RDM, which has been ongoing since at least 2014 through the development of 6-155mm large-caliber ammunition, under a scheme that includes the appointment of Pindad as the RDM manufacturing hub for the Asia Pacific, the exchange of experts for technology transfer, and a co-manufacturing plan at Pindad's facility in Turen, Malang. In 2024, the relationship was strengthened through a Head of Agreement covering the strategic supply of 40mm caliber ammunition propellants and components, technology transfer, transfer of manufacturing facilities, and revitalization of Pindad's large-caliber ammunition filling plant.[44]

This pattern deepened when PT Dahana, a state-owned enterprise (BUMN) also a member of DEFEND ID, signed an MoU with RDM in November 2025 for the construction of an energetic material facility in Indonesia. Under the scheme, RDM acts as a technology provider and is committed to technology transfer, while the planned facility at Dahana's Energetic Material Center in Subang will produce the energetic materials needed for large-caliber munitions and warhead fillings, while also having a dual-use function for the mining industry.[45] From a military-industrial complex perspective, the Pindad–Dahana–RDM relationship demonstrates the formation of a cross-border defense industry network connecting state-owned enterprises, foreign defense companies, technology transfer, production facilities, economic diplomacy interests, and market expansion. Africa itself is increasingly seen as one of Indonesia's strategic industrial expansion spaces. At the 2024 Indonesia Africa Forum, the government noted PT Pindad's collaboration with RDM in South Africa, while PT Dirgantara Indonesia also expanded its business relations with the Democratic Republic of Congo and Senegal.[46]

---

[42] Indonesia Defense, "Spesifikasi Drone Baru untuk Tugas Operasi Prajurit Marinir di Perbatasan," April 17, 2024, https://indonesiadefense.com/spesifikasi-drone-baru-untuk-tugas-operasi-prajurit-marinir-di-perbatasan/, accessed September 8, 2026.

[43] Rheinmetall explains that RDM is jointly owned by Rheinmetall Waffe Munition GmbH (51 percent) and Denel (Pty) Ltd., and is engaged in the production of medium and large caliber ammunition, artillery and mortar systems. See Rheinmetall, "Rheinmetall Denel Munition (Pty) Ltd.," https://www.rheinmetall.com/en/company/subsidiaries/rheinmetall-denel-munition.

[44] PT Pindad (Persero), "Pindad Bersiap Menjadi Produsen Munisi Global," August 8, 2014, https://pindad.com/pindad-bersiap-menjadi-produsen-munisi-global.

[45] PT Dahana, "Dahana–RDM Sepakati Pembangunan Fasilitas Energetic Material di Indonesia," November 25, 2025, https://dahana.id/id/dahana-rdm-sepakati-pembangunan-layanan-energetic-material-di-indonesia/.

[46] Ministry of Foreign Affairs of the Republic of Indonesia, "Indonesia dan Negara-Negara Afrika Tandatangani MoU Industri Strategis di IAF 2024," September 3, 2024, https://kemlu.go.id/berita/indonesia-dan-negara-negara-afrika-tandatangani-mou-industri-strategis-di-iaf-2024.

Upon further investigation, we discovered that the Indonesian state-owned defense company's partnership with Rheinmetall Denel Munition (RDM) raises concerns. This partnership needs to be examined through the company's global supply chain track record. A 2020 Open Secrets investigation documented that RDM exported 120mm mortar munitions to Saudi Arabia and the United Arab Emirates, two key members of the military coalition in Yemen. The investigation also found that ammunition fragments recovered after the 2018 attack on Hodeida, which killed and injured civilians, were found to have a number of characteristics similar to RDM's 120mm mortars. These findings do not, in themselves, prove RDM's legal responsibility for the attack, but they do highlight fundamental issues regarding end-user control and the company's ability to ensure that exported products are not used in human rights or humanitarian law violations. The controversy even prompted tightening of South African export licensing in 2019, including demands for end-user inspections, which temporarily halted export permits to Saudi Arabia and the UAE.[47]

Similar risks have resurfaced in the Sudanese conflict. In July 2025, the Sunday Independent reported allegations from the Sudanese Military Capabilities platform that the 40mm PHOS M8931 phosphorus ammunition allegedly used by the Rapid Support Forces (RSF) in the fighting in Khartoum could be traced to the production lines of the American Rheinmetall Munitions and RDM.[48] Broader issues also arise within Rheinmetall's corporate network. In a May 2024 communication to Rheinmetall AG, several UN Special Rapporteurs and independent experts stated that they received information that the company continued to supply Israel with hundreds of thousands of precision tank ammunition after October 7, 2023, despite the lack of public information, according to the experts, demonstrating the implementation of adequate enhanced human rights due diligence to assess the risks of using these weapons in the Gaza conflict. In June 2024, the UN experts then specifically included Rheinmetall AG among the arms manufacturers requested to halt transfers to Israel due to the risk of complicity in serious violations of human rights and humanitarian law. It is important to distinguish that the UN communication was addressed to Rheinmetall AG, not RDM, even though RDM is a joint venture 51 percent owned by Rheinmetall Waffe Munition, part of the Rheinmetall Group.[49]

This track record makes Indonesia's cooperation with RDM more than just a matter of technology transfer and defense industry independence. PT Pindad was previously designed to be RDM's manufacturing hub for the Asia Pacific region, while in 2025, PT Dahana signed another collaboration with RDM to build an energetic materials facility in Indonesia. As Indonesia is increasingly positioned as a production base and potential supplier for the regional and global market, human rights risks no longer stop at how technology is used by the TNI, but extend to who buys products made in Indonesia, to whom those products are then transferred, and for what operations those products are ultimately used.

At this point, the contemporary military-industrial complex has become more complex than the classic configuration criticized by Eisenhower in 1961. The problem no longer rests on the relationship between the military, the government, and the industries that benefit from increased spending and arms production within a single country. Today's defense industry operates through transnational supply chains, with technology developed in partnership with foreign companies, components and raw

[47] Zen Mathe and Caryn Dolley, "Unaccountable 0004: Rheinmetall Denel Munition: Murder and Mayhem in Yemen," Open Secrets, January 22, 2020, https://www.opensecrets.org.za/rheinmetall-denel-munition-murder-and-mayhem-in-yemen/.

[48] Manuel Godsin, "Rheinmetall Denel Faces Scrutiny over Allegations of Arms Use in Sudan Conflict," *Sunday Independent/The Star*, July 8, 2025, https://thestar.co.za/sundayindependent/news/2025-07-08-rheinmetall-denel-faces-scrutiny-over-allegations-of-arms-use-in-sudan-conflict/.

[49] United Nations Human Rights Council, Special Procedures, "Communication to Rheinmetall AG," Ref. AL OTH 81/2024, 17 May 2024, 4, https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=29082

materials produced across borders, knowledge transferred through technology transfer, and the final products re-marketed to other countries.

As Indonesian state-owned defense enterprises are pushed to increase production capacity while expanding international markets, a new risk arises that weapons, ammunition, energetic materials, drones, surveillance devices, and dual-use technology produced or supplied in Indonesia will ultimately be used by purchasing countries for actions that violate human rights or international humanitarian law. Therefore, the Indonesian military-industrial complex is better understood not as a purely domestic system, but as a transnational ecosystem that seeks to build domestic production capacity while positioning the Indonesian defense industry within the global arms market and supply chain.

3. What is the Human Rights Impact of the Military's Use of Surveillance Technology?

In his book, The Rise of the Network Society (2010), Manuel Castells asserts that the reality of technological development has brought humanity into an era known as the digital age. Castells equates the current technological revolution to a historical event of equal magnitude with the Industrial Revolution of the 18th century, as both have triggered significant, pervasive changes, penetrating all spheres of human activity. The core of the transformation we are experiencing in this current revolution is information processing and communication technology.[50]

From a security and defense perspective, technological developments, particularly in the global defense and military sectors, have given rise to the concept of the Internet of Military Things (IoMT) or Battlespace Internet of Things (BIoT). This concept describes the use of a network of internet-connected devices and the actors operating within them. The Australian Defence Force (ADF) has even invested in infrastructure and systems for command and control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems to collect, analyze, and disseminate information.[51]

Furthermore, this technological transformation has also been adapted. It has created a new space within the global security dynamic known as cyberspace. The emergence of cyberspace as a new domain of human-state interaction has also revolutionized the way information is gathered and surveillance practices are conducted, making cyberspace a new strategic arena for states to protect digital sovereignty, vital infrastructure, and national interests.

[50] Manuel Castells, *The Rise of the Network Society*, 2nd ed. (Chichester: Wiley-Blackwell, 2010), 29–30.
[51] Claire Withrington, "The Internet of Military Things," August 24, 2023, https://cove.army.gov.au/article/internet-military-things.

Figure 1. How Cyberspace Is at the Leading Edge of Global Change



Source: The Diplomat

The image above shows cyberspace connecting all countries, regardless of territorial boundaries. This situation, on the one hand, creates uncertainty in terms of security. Even at the 2016 Munich Security Conference (MSC), attended by world leaders, they called for an agreement on norms of behavior in cyberspace. More than 20 countries have agreed that they should not attack each other's critical infrastructure during peacetime. Corporate norms are still in their infancy, but they may include a policy of not withholding security updates from any customer, wherever they are located.[52]

Developments in information and communication technology have fundamentally transformed the way intelligence agencies operate. While during the Cold War, intelligence relied on physical operations, infiltration, and field data collection, in the digital era, intelligence has shifted to a data-driven paradigm. One of the most prominent aspects of this development is the increasing use of surveillance technology as a key instrument in cybersecurity and defense architecture.

In the global landscape, increased surveillance of individuals, groups, or countries of concern has been under increasing scrutiny since September 11, 2001, or the 9/11 attacks in New York City, United States. Even CENTCOM (United States Central Command),[53] requested the assistance of the RAND Corporation in developing instruments to measure the effectiveness of intelligence, surveillance, and reconnaissance operations to evaluate current performance and plan, influence, and provide resources for future operations.[54]

---

[52] B. McConnell, "How Cyberspace Is at the Leading Edge of Global Change," *The Diplomat*, February 25, 2016, https://thediplomat.com/2016/02/how-cyberspace-is-at-the-leading-edge-of-global-change.

[53] CENTCOM is the United States military command responsible for the region encompassing much of the Middle East, Central Asia, and Africa. Its primary mission is to defend and promote U.S. interests in the region, which includes military operations, humanitarian assistance, and joint exercises with partner nations. See US Central Command, "About Us," https://www.centcom.mil/ABOUT-US/.

[54] David Luckey et al., *Measuring Intelligence, Surveillance, and Reconnaissance Effectiveness at the United States Central Command* (Santa Monica, CA: RAND Corporation, 2021).

The militarization of technology is now a key focus in efforts to strengthen the defense capabilities of various countries. The United States Department of Defense (DoD) is expected to allocate approximately US$384 billion, equivalent to Rp6,424 trillion, as part of its national security strategy aimed at modernizing all branches of the military and increasing investment in defense research and development (R&D).[55]

According to the Investing in Defense Part III report released by Visual Capitalist in collaboration with Global X ETFs, total US spending on defense technology in fiscal year 2026 is projected to increase by 71 percent compared to 2020—from US$162.3 billion to US$278 billion. This surge reflects the US military's strong push to adopt high-tech defense systems that integrate artificial intelligence (AI), big data processing, and autonomous technologies in land, sea, and air operations.[56]

The UK is also accelerating its defense innovation efforts. The UK government has committed to increasing defense spending to 2.5% of GDP starting in 2027, with a long-term aspiration of 3.5% of GDP for "core" defense spending and 1.5% for "resilience and security" by 2035, totaling 5% of national income for national security. This significant increase will encourage investment in areas such as drone technology, laser weapon systems, long-range weapons, and advanced ammunition.[57]

In the Indonesian context, the adaptation of defense strengthening to the cyberspace locus is also evident. Within the framework of Law No. 3 of 2002 concerning National Defense, cyberspace has not been included in the focus. This is because in the explanation of the said Law, the scope of problems related to globalization only includes terrorism, illegal immigration, the dangers of narcotics, theft of natural resources, piracy, and environmental destruction. However, through Law No. 23 of 2019 concerning Management of National Resources for National Defense, Article 4 paragraphs (2) and (3) it has been explained that cyber attacks have been mentioned as a form of threat.

In the context of defense, especially ISR (Intelligence, Surveillance, and Reconnaissance), it is necessary to understand that its existence has a significant role for the military in its efforts to maintain national defense.[58] ISR work, which includes the collection, analysis, and dissemination of information, helps decision-making in defense, security, and crisis response operations, thus enabling the military to detect threats and respond effectively to various developing scenarios.[59] However, the strengthening of cyberspace and the use of surveillance technology builds a debate on the ethics of the implications of the reach of state security intelligence that focuses on efforts to balance individual rights, freedoms, and privacy with state security.[60]

---

[55] Elvan Widyatama, "Gila-Gilaan! AS Habiskan Rp6.000 T Buat Teknologi Perang Masa Depan," CNBC Indonesia, November 13, 2025, https://www.cnbcindonesia.com/research/20251112105824-128-684492/gila-gilaan-as-habiskan-rp6000-t-buat-teknologi-perang-masa-depan.

[56] Widyatama, "Gila-Gilaan! AS Habiskan Rp6.000 T Buat Teknologi Perang Masa Depan."

[57] Timo Stellpflug, "The Resurgence of European and UK Defense Tech: Markets, Technology, and Investment," *Taylor Wessing*, July 31, 2025, https://www.taylorwessing.com/en/interface/2025/defence-tech/the-resurgence-of-european-and-uk-defence-tech.

[58] ISR consists of three complementary components. Intelligence is the gathering of processed and analyzed information. Surveillance is the continuous monitoring of an area, individual, or activity over time. Reconnaissance is the gathering of specific information about a particular area, object, or threat, often under time-sensitive conditions. Furthermore, reconnaissance missions play a vital role in verifying other intelligence. See Elistair, "Intelligence, Surveillance, and Reconnaissance (ISR)," https://elistair.com/glossary/intelligence-surveillance-reconnaissance/.

[59] Elistair, "Intelligence, Surveillance, and Reconnaissance (ISR)."

[60] Adam Henschke, *Ethics in an Age of Surveillance: Personal Information and Virtual Identities* (Cambridge: Cambridge University Press, 2017); Laura Muir, "Control Space?: Cinematic Representations of Surveillance Space between Discipline and Control," *Urban Surveillance* 9, no. 3 (2012): 263–279.

This discourse arose because technological developments, initially oriented towards strengthening national security, also have the potential for abuse. Power, information, and control are intertwined in cyberspace. This is because the technology in question is used by those in power as an invasive surveillance tool that intrudes on citizens' privacy, resulting in various forms of human rights violations.

Figure 2. The Use of Black Faces in Facial Recognition Systems



Source: epic.org

The image above shows that many Chinese technology companies continue to export their facial recognition technology to African markets while supporting domestic surveillance practices that include the detection of Uyghurs and other ethnic minorities. Facial recognition technology, once considered a potential solution to social challenges such as crime, is now widely criticized for its racial bias and the risks it poses to privacy and civil liberties.[61]

Peron, A.E. dos R., Almstadter Mattar de Magalhães, D., & Caetano, G.F. (2025), introduced the concept of techno-authoritarianism as the convergence of authoritarianism and technology. This concept was adopted considering the increasingly close relationship between authoritarianism and various technological devices that can cause rifts in democracy. This term can also describe and understand the extensive use of technological resources that undermine the principles of democracy and human rights.[62]

Because governments around the world have essentially been using AI-based surveillance systems disguised as "intelligent" methods for control. However, its use, which aligns with institutional and democratic disruption, actually creates forms of repression against those who oppose the government.[63]

[61] B. Jili, "The Rise of Chinese Surveillance Technology in Africa," Electronic Privacy Information Center (EPIC), May 31, 2022, https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa/.
[62] AE dos R. Peron, D. Almstadter Mattar de Magalhães, and G.F. Caetano, "Beyond Digital Repression: Techno-Authoritarianism in Radical Right Governments," *Cogent Social Sciences* 11, no. 1 (2025), https://doi.org/10.1080/23311886.2025.2528457.
[63] Peron, Magalhães, and Caetano, "Beyond Digital Repression."

3.1. Violations of Freedom of Opinion, Expression, and Assembly

3.1.1. Guarantee of Freedom of Opinion, Expression, and Assembly

The Constitution through Article 28 E paragraph (3) of the 1945 Constitution states "Everyone has the right to freedom of association, assembly, and expression of opinion." This guarantee is detailed in Law No. 9 of 1998 concerning Freedom of Expression of Opinions in Public. In the considerations of letters a and b, the said Law emphasizes that freedom of expression of opinion in public is a human right guaranteed by the 1945 Constitution and the Universal Declaration of Human Rights, then the freedom of every citizen to express opinions in public is a manifestation of democracy in the order of life in society, nation, and state.

Furthermore, a number of norms in the said law further emphasize the guarantee of freedom of expression for every citizen, as well as being part of democratic rights. Article 2 paragraph (1) states that every citizen, individually or in groups, can express their opinion as a manifestation of democratic rights and responsibilities in social, national, and state life. Article 5 also emphasizes that citizens who express their opinions in public have the right to express their thoughts freely and receive legal protection.

Although freedom of expression is legally classified as a derogable right—that is, a right that can be restricted under certain conditions—this derogable nature does not necessarily reduce its fundamental meaning in a democratic system. In the context of national law, these restrictions are regulated, among other things, in Article 9 paragraph (2) of Law Number 9 of 1998, which stipulates that the expression of opinions cannot be carried out in certain places in order to maintain public order, safety, and the strategic interests of the state. These restrictions, in theory, are a form of procedural regulation that aims to harmonize the use of rights with the broader public interest.

However, the basic principle must still be emphasized: the right to express opinions in public is a protected constitutional right of citizens, not a privilege given by the state that can be arbitrarily revoked. Within the framework of human rights law, the fact that a right can be restricted does not mean that the state has absolute freedom to intervene. Restrictions are only valid if they meet the principles of legality, proportionality, and legitimate aim as stated in Article 19 paragraph (3) of the International Covenant on Civil and Political Rights (ICCPR), which Indonesia has ratified.

In other words, although the right to express opinions can be regulated, it cannot be eliminated. This right remains inherent in every citizen as a core democratic right that is the basis for the continuity of an open, accountable, and responsive government. This is evident through the construction of Article 7 of Law No. 9 of 1998 which emphasizes the obligations and responsibilities of government officials regarding the implementation of public expression of opinions by citizens, namely: (a) protecting human rights; (b) respecting the principle of legality; (c) respecting the principle of the presumption of innocence; and (d) providing security.

More fundamentally, Law No. 39 of 1999 concerning Human Rights provides a firm normative foundation for the position of human rights within the Indonesian legal system. Article 2 of this law states that the state recognizes and upholds human rights and basic human freedoms as rights inherent in and inseparable from human beings. This formulation demonstrates that the state does not have the authority to "grant" or "remove" these rights, as human rights do not originate from the state, but from human nature itself. The state is only obligated to protect, respect, and uphold these rights for the sake of human dignity, welfare, happiness, intelligence, and justice for all citizens.

If a state fails to comply with these principles, restrictions become violations, and the state acts contrary to its constitutional mandate and national human rights law. Furthermore, in a contemporary context marked by the increasing militarization of cyberspace, the principles in

Article 2 become even more important. The use of various digital surveillance technologies, cyber surveillance mechanisms, and the expansion of security apparatus powers are often carried out in the name of national security stability. However, without strict oversight, these practices can easily turn into forms of control that stifle freedom of expression and erode citizens' privacy.

3.1.2. Techno-Authoritarianism: When Technology Is Used as an Instrument to Violate Human Rights

Paradigmatically, the militarization of cyberspace management is a manifestation of the concept of techno-authoritarianism, which emphasizes the control and surveillance of cyberspace under the guise of defense, security, or stability. When a state adopts a militaristic logic in managing cyberspace, particularly through a repressive defense and security approach, the space has the potential to lose its democratic character. The transformation of digital space into a domain that is monitored, controlled, and protected by militaristic methods that do not place human rights principles as fundamental. As a result, digital technology has provided authoritarian governments with new tools to control, silence, and punish dissent across borders. Digital technology allows regimes to monitor and respond to the political activities of their citizens within their jurisdiction, but also to diaspora communities abroad. Thus, digital technology has become a crucial component in the apparatus of transnational repression.[64]

Figure 3. Digital Authoritarianism in the Middle East



Source: thesecuritydistillery.org

Techno-authoritarianism is also a phenomenon in the Middle East, although the term used is digital authoritarianism.[65] Over the past ten years, governments in several Middle Eastern countries have used digital information and communication technologies as a tool to strengthen control over their citizens. Drawing inspiration from models set by China, Russia, and Israel,

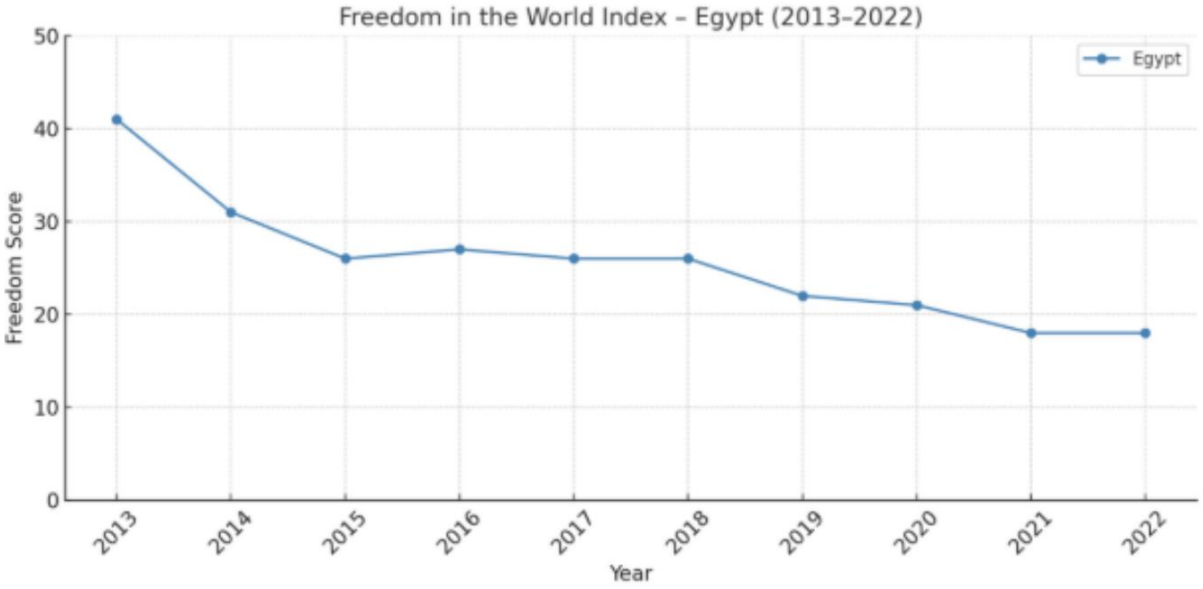
[64] Marcus Michaelsen, *The Digital Transnational Repression Toolkit, and Its Silencing Effects* (Freedom House, 2020), https://freedomhouse.org/report/special-report/2020/digital-transnational-repression-toolkit-and-its-silencing-effects.

[65] The Brookings Institution defines digital authoritarianism as "the use of digital information and communications technologies by authoritarian and autocratic states to monitor, manipulate, repress, and control populations." See Alina Polyakova and Chris Meserole, *Exporting Digital Authoritarianism: The Russian and Chinese Models* (Washington, DC: Brookings Institution, 2019).

Middle Eastern governments have implemented policies and strategies aimed at censorship, digital deception, and mass surveillance that have worsened the region's human rights record.[66]

For example, in Egypt, as internet usage increases in Egypt, the government's efforts to control the digital space and impose stricter oversight of the society is also increasing. The Human Rights Watch website was blocked by Egyptian authorities just a day after the organization released a report on systematic torture in the country's prisons.[67] The Freedom House Index shows that average internet freedom has declined by about 40% in Egypt.

Figure 4



Source: Freedom House, 2022

The Freedom House index shows that Egypt has experienced a decline in freedom of expression and belief, the right to organize and associate, the rule of law, and personal autonomy and individual rights.[68] The Egyptian government focuses on four domains: a restrictive legal framework, internet censorship, urban surveillance, and SDIOs (Social Media Information Organizations). By exploiting these four domains, the Egyptian government has built a comprehensive system of digital authoritarianism. This system not only strengthens its grip on power but also serves as a blueprint for other authoritarian regimes seeking to use digital technology to suppress dissent and maintain control.[69]

In the context of a restrictive legal framework, the provisions in Egypt are:

1. A law requiring internet service providers to establish real-time traffic monitoring and recording systems on their networks. This would allow for continuous monitoring of online activity;
2. Legal frameworks that penalize online freedom of speech under the guise of protecting national identity and culture and preventing defamation. This often results in the suppression of dissenting opinions and freedom of expression.

---

[66] Giorgia Piovesan, "Digital Authoritarianism in the Middle East," *The Security Distillery*, April 19, 2023, https://thesecuritydistillery.org/all-articles/digital-authoritarianism-in-the-middle-east.

[67] Al Jazeera, "Egypt Blocks Human Rights Watch Website," September 8, 2017, https://www.aljazeera.com/news/2017/9/8/egypt-blocks-human-rights-watch-website.

[68] Freedom House, "Egypt," Freedom on the Net 2022, 2022, https://freedomhouse.org/country/egypt/freedom-net/2022.

[69] Ihsan Yilmaz, Ali Mamouri, Shahram Akbarzadeh, and Muhammad Omer, *Authoritarian Diffusion in the Cyberspace: How Egypt Learns, Emulates, and Cooperates in Digital Authoritarianism* (Brussels: European Center for Populism Studies, 2025), May 9, 2025, https://doi.org/10.55271/rp0097.

3. VPN restrictions, following in the footsteps of countries like China and Russia in banning or restricting the use of Virtual Private Networks (VPNs). Although VPNs are technically legal in Egypt, many VPN servers and websites are blocked, hindering their practical use; and
4. Control over social media companies using various methods, such as threatening companies with bandwidth restrictions and outright bans if they fail to comply with government requests.[70]

Egypt even has a 2018 Cybercrime Law that treats all social media accounts with more than 5,000 followers as media outlets, making them eligible for censorship.[71] The law also requires internet service providers to establish systems that allow for real-time monitoring and recording of traffic on their networks.[72] The cybercrime law criminalizes any form of speech that is contrary to national security, and allows for searches of citizens' personal devices and the blocking of social media accounts without judicial authorization, on the grounds of spreading false information or inciting unlawful activity.[73]

Meanwhile, in the Indonesian context, digital authoritarianism is a manifestation of the ongoing militarization of cyberspace. Nearing three decades after the 1998 Reforms, Indonesian civil society still faces serious challenges: strengthening authoritarianism, repression of freedom of expression, and the misuse of technology to control narratives and marginalize critical voices. This repression has triggered various forms of violations of freedom of opinion, expression, and association.[74]

[70] Marwa Fatafta, "Egypt's New Data Protection Law: Data Protection or Data Control?" Access Now, September 24, 2020, https://www.accessnow.org/egypts-new-data-protection-law-data-protection-or-data-control/.
[71] Reporters Without Borders (RSF), "Egypt's New Cybercrime Law Legalizes Internet Censorship," August 21, 2018, https://rsf.org/en/egypt-s-new-cybercrime-law-legalizes-internet-censorship.
[72] Privacy International, "State of Privacy: Egypt," January 26, 2019, https://www.privacyinternational.org/state-privacy/1001/state-privacy-egypt.
[73] Ihsan Yilmaz, Ali Mamouri, Shahram Akbarzadeh, and Muhammad Omer, "Authoritarian Diffusion in the Cyberspace: How Egypt Learns, Emulates, and Cooperates in Digital Authoritarianism," *European Center for Populism Studies*, May 9, 2025, https://www.populismstudies.org/authoritarian-diffusion-in-the-cyberspace-how-egypt-learns-emulates-and-cooperates-in-digital-authoritarianism/.
[74] See LP3ES, "Membangun Resiliensi Masyarakat Sipil Setelah 27 Tahun Reformasi," May 22, 2025, https://www.lp3es.or.id/2025/05/22/membangun-resiliensi-masyarakat-sipil-setelah-27-tahun-reformasi/.

Figure 5. Cartoon of Restrictions on Freedom of Opinion and Expression



Source: Radioidola

The condition of digital authoritarianism in Indonesia is reflected in the last five years, 2020–2024, when the internet freedom score according to Freedom House tends to stagnate and is consistently in the Partly Free category, indicating that a country, in this case Indonesia, has increasing internet access, but still faces significant challenges to online freedom, including restrictions, censorship, and attacks on users.[75]

Table 1. Internet Freedom Score in Indonesia 2020-2024

No	Year	Score	Issues Highlighted
1	2020	49/100	Increased disinformation and pro-government propaganda, as well as technical attacks against activists, journalists, and civil society groups. The government also again restricted Internet access, including the disruption of connectivity in Papua and West Papua in August–September 2019 amidst a wave of protests. Although declared unlawful by the courts, these practices demonstrate a trend toward using digital control as a political response. At the same time, the criminalization and harassment of online criticism continue to narrow the space for freedom of expression in the digital realm.[76]
2	2021	48/100	The emergence of new regulations requiring content removal and registration for technology companies has impacted online freedom of expression. Internet access in Papua has been disrupted again, including during sensitive moments related to independence issues. At the same time, government critics, journalists, and ordinary internet users continue to face criminal charges and harassment for their online

[75] Scores are based on a scale of 0 (least free) to 100 (most free). These categories include: below 35 is "Not Free," 35-69 is "Partly Free," and 70-100 is "Free."

[76] Freedom House, "Indonesia: Freedom on the Net 2020 Country Report," 2020, https://freedomhouse.org/country/indonesia/freedom-net/2020.

			activities. Technical attacks against journalists, media outlets, and think tanks have also increased as they cover critical issues.[77]
3	2022	49/100	Internet access in Papua was disrupted again, including during moments related to the issue of Papuan independence. In the digital space, criticism of the government continued to be met with criminal prosecutions, harassment, and increased technical attacks against journalists, media outlets, and think tanks. Outside of the reporting period, authorities also tightened registration and content removal requirements for technology companies, which resulted in the temporary blocking of several platforms.[78]
4	2023	47/100	Internet freedom in Indonesia has worsened, particularly due to the implementation of Ministerial Regulation No. 5 of 2020, which expanded the content moderation regime and threatened freedom of expression and user privacy. In June 2022, the government temporarily blocked several platforms that failed to comply with registration requirements. Meanwhile, government critics, journalists, and internet users continue to face criminalization, violence, and online harassment, while internet access disruptions in Papua continue to occur.[79]
5	2024	49/100	Online hate campaign against Rohingya refugees and the spread of disinformation increased sharply in the run-up to the February 2024 elections. At the same time, government critics, journalists, and internet users continued to face criminal prosecution, violence, and harassment in retaliation for their online activities. Political and economic elites, including actors linked to major parties and the military, also manipulated public opinion on social media through the use of paid buzzers.[80]

Source: Freedom House 2020-2024

Freedom House's findings from 2020 to 2024 demonstrate that the decline in internet freedom in Indonesia is not an isolated incident, but rather part of a gradually consolidating trajectory of digital authoritarianism. The state has not completely shut down digital access, but has systematically developed legal, technical, and political tools to control the flow of information, shape public opinion, and limit critical expression, particularly during sensitive moments.

The practice of disrupting and restricting internet access, particularly in Papua, has become a recurring pattern year after year. Access cuts are not merely an emergency response, but rather a regional-based information control strategy. Pressure on critical actors—journalists, activists, researchers, and ordinary internet users—has been a consistent element throughout the 2020–2024 period. Criminalization, online harassment, technical attacks, and even physical violence serve to create a chilling effect, leading citizens to self-censor. Even as the 2024 elections approach, another dimension of digital authoritarianism is becoming increasingly apparent, namely the manipulation of discourse through organized disinformation and paid buzzers.

[77] Freedom House, "Indonesia: Freedom on the Net 2021 Country Report," 2021, https://freedomhouse.org/country/indonesia/freedom-net/2021.
[78] Freedom House, "Indonesia: Freedom on the Net 2022 Country Report," 2022, https://freedomhouse.org/country/indonesia/freedom-net/2022.
[79] Freedom House, "Indonesia: Freedom on the Net 2023 Country Report," 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023.
[80] Freedom House, "Indonesia: Freedom on the Net 2024 Country Report," 2024, https://freedomhouse.org/country/indonesia/freedom-net/2024.

The impact of digital authoritarianism in Indonesia is also evident in a survey conducted by LP3ES of 1,658 civil society organizations (CSOs). The survey revealed that 31% of civil society organizations experienced digital threats and repression in various forms, such as hacking, phishing, and intimidation. Interestingly, the survey found two emerging patterns: (1) a high prevalence of threats in urban and industrial areas such as Jakarta, West Java, and Central Java, and (2) digital attacks emerging in mineral-rich regions such as East Kalimantan, Central Sulawesi, and Maluku.[81]

Technological developments, however, come with a dark side and are wielded by those in power. There are three main patterns of digital repression in Indonesia. Two of these are even vulnerable to, or potentially, involving, security actors. These patterns are:

1. Cyber terror in all its forms, from hacking, social media account takeovers, internet activity surveillance, to constant calls from various unknown numbers;
2. Criminalization using ambiguous articles in laws and regulations related to the internet, in this case one of the laws that is often used is Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE), especially Article 27 Paragraph 3 concerning defamation and Article 28 Paragraph 2 concerning hate speech.[82]

Amnesty International's report also states that the misuse of surveillance technology, as well as the use of technology that is inconsistent with human rights, such as highly invasive spyware, are some of the many tactics used worldwide to narrow public space. At the same time, human rights defenders and activists have repeatedly faced online repression in Indonesia, one of which is through Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions.[83] This condition is evident in data from Amnesty International Indonesia, which recorded 527 cases of violations of freedom of expression based on the ITE Law against at least 560 citizens from 2019 to 2024. Of these, 421 cases, with 449 victims, have received court sentences.[84]

Furthermore, it's equally important to view this issue within a gender mainstreaming framework. Women and other gender-based groups often experience multiple vulnerabilities due to increasingly intensive and opaque surveillance practices. Digital surveillance also has the potential to increase the risk of online gender-based violence, such as doxing, digital harassment, intimidation, and the criminalization of expression, which impacts women's participation in public and political spaces.

Biometric technologies, including facial recognition, fingerprint scanning, and iris detection, are increasingly integrated into surveillance systems, raising critical concerns about privacy and equity. Gender plays a crucial role in the implementation and impact of these technologies, as biases embedded in biometric systems disproportionately affect women, non-binary individuals, and marginalized communities. The intersection of gender and surveillance reveals structural

[81] LP3ES, "Membangun Resiliensi Masyarakat Sipil Setelah 27 Tahun Reformasi."
[82] Wijayanto, "Masyarakat Sipil dan Represi Digital," *Kompas*, June 10, 2025, https://www.kompas.id/artikel/melindungi-masyarakat-sipil-dari-represi-digital-2.
[83] Amnesty International, "Unravelling a Murky Network of Spyware Exports to Indonesia," May 17, 2024, https://www.amnesty.org/en/latest/news/2024/05/unravelling-a-murky-network-of-spyware-exports-to-indonesia/.
[84] Amnesty International Indonesia, "'Arus Balik' Hak Asasi Manusia di 100 Hari Pemerintahan Baru," January 21, 2025, https://www.amnesty.id/kabar-terbaru/siaran-pers/arus-balik-hak-asasi-manusia-di-100-hari-pemerintahan-baru/01/2025/.

inequalities, where algorithmic biases in biometric identification often misidentify or exclude certain groups, reinforcing existing social inequalities.[85]

This issue was also recently highlighted during a cyber patrol conducted by the Indonesian National Armed Forces (TNI) Cyber Unit during the August 2025 demonstrations, which uncovered several alleged criminal acts. One result of the patrol was the visit of the Cyber Unit Commander (Dansat Siber) of TNI Headquarters and several high-ranking TNI officers to the Jakarta Metropolitan Police (Polda Metro Jaya) for consultations regarding alleged criminal acts committed by Malaka Project CEO Ferry Irwandi.

Meanwhile, Law No. 3 of 2025 concerning the TNI, in Article 7 paragraph (2) letter b has mandated one of the TNI's duties in Military Operations Other Than War (MOOTW) related to the cyber sector, namely assisting in cyber defense threat efforts, but in the explanation of the related provisions, it has been emphasized that the context of the cyber threat in question is in the defense sector (cyber defense), not those related to law enforcement. This step actually has the potential to become an instrument for controlling public narratives, worsening the shrinking civil space trend that has become a concern for national and international civil society, and opening up the legitimacy of repressive actions against civilians in the digital space.[86]

This situation has been a concern for various elements of civil society since the beginning, as an implication of the revision of Law No. 34 of 2004 concerning the Indonesian National Armed Forces (TNI). One example is the TNI's expanded role in the OMSP, supporting the government in addressing cyber threats. The government's Problem Inventory List (DIM) explains that:[87]

> "...Cyberwarfare not only attacks physical infrastructure, but also the virtual and cognitive dimensions. Enemies/opponents engage in social manipulation, information pollution, and narrative reinforcement with exaggerated expressions to attack cognitive vulnerabilities. Conflicts that exploit this information advantage become a highly dangerous weapon, influencing people's beliefs, attitudes, and behavior, resulting in social, political, and economic conflict that ultimately threatens national security."

This issue strongly suggests that the militarization of cyberspace is occurring as a consequence of the revision to the TNI Law. This militarization of cyberspace is the state's attempt to construct the cyber domain as a primary threat to national security, thereby legitimizing the implementation of military-oriented measures to address cyber threats and justifying the ongoing and relentless development and enhancement of cyber military capabilities.[88]

In the Draft Cyber Security and Resilience Bill (RUU KKS), ELSAM has also emphasized that several provisions in the a quo bill have the potential to pave the way for the militarization of digital space in Indonesia by expanding the role and authority of security forces in monitoring citizens' online activities. This situation creates an ideal ecosystem for the militarization of technology. The bill's approach is too state-oriented, rather than focused on individual security and citizen protection.[89]

---

[85] Rubina Shaheen, "Gender and Surveillance: The Implications of Biometric Technologies for Privacy and Equity," Journal of Gender, Power, and Social Transformation 1, no. 3 (2024).

[86] SETARA Institute, "Patroli Siber TNI Mengarah pada Represi Digital," September 9, 2025, https://setara-institute.org/patroli-siber-tni-mengarah-pada-represi-digital/.

[87] Southeast Asia Freedom of Expression Network (SAFEnet), "Pernyataan Sikap SAFEnet: Tolak RUU TNI, Tolak Militerisasi Ruang Siber," March 17, 2025, https://safenet.or.id/id/2025/03/tolak-ruu-tni-tolak-militerisasi-ruang-siber/.

[88] SAFEnet, "Pernyataan Sikap SAFEnet: Tolak RUU TNI, Tolak Militerisasi Ruang Siber."

[89] ELSAM, "Peneliti ELSAM Peringatkan Potensi Militerisasi Ruang Digital lewat RUU Keamanan dan Ketahanan Siber (RUU KKS)," October 21, 2025, https://www.elsam.or.id/teknologi-dan-ham/peneliti-elsam-peringatkan-potensi-militerisasi-ruang-digital-lewat-ruu-keamanan-dan-ketahanan-siber–ruu-kks-.

Such conditions demonstrate the paradox of democracy, particularly regarding the rights to freedom of opinion, expression, and assembly guaranteed by the Constitution through Article 28 E paragraph (3) of the 1945 Constitution which states "Everyone has the right to freedom of association, assembly, and expression of opinion." It should be understood that the birth of freedom of expression aims to eliminate restrictions in conveying certain opinions or views that have a negative impact on the welfare and justice of society. Freedom of expression is used to convey views and opinions, both between individuals or groups.[90]

3.2. Violation of Citizens' Privacy

3.2.1. Guarantee of Citizens' Privacy

Regulatory arrangements that guarantee citizens' privacy are becoming increasingly urgent amidst the massive digitalization of public services, data collection by the state and corporations, and the use of surveillance technology. ELSAM also emphasized that in the context of personal data, the most important thing is to have instruments to strengthen the protection of citizens' personal data through a robust legal framework. The focus of the debate is also not on traditional sovereignty discourse (territoriality and jurisdiction), but rather on the sovereignty of individual data owners.[91]

Figure 6. Illustration of the Urgency of a Legal Umbrella for Personal Data Protection



Source: ELSAM

Privacy is not merely a technical issue, but rather a prerequisite for freedom of expression, freedom of opinion, and democratic participation. Therefore, clear, accountable, and citizen-friendly privacy regulations are an essential foundation for preventing digital authoritarian practices and maintaining the quality of democracy. Article 28G paragraph (1) of the 1945 Constitution affirms that everyone

[90] Alifah Jasmine Kallista Remanu et al., "Analisis Implikasi UU ITE terhadap Kebebasan Berekspresi di Ruang Digital: Studi Kasus Greenpeace Indonesia," *Jurnal ISO: Jurnal Ilmu Sosial, Politik dan Humaniora* 4, no. 2 (2024).

[91] ELSAM, "UU Perlindungan Data Pribadi Mendesak untuk Menjamin Kedaulatan Individu di Ruang Siber," 2025, https://www.elsam.or.id/siaran-pers/uu-perlindungan-data-pribadi-mendesak-untuk-menjamin-kedaulatan-individu-di-ruang-siber.

has the right to protection of themselves, their families, their honor, their dignity, and their property. This is further elaborated in several applicable regulations, including the following:[92]

a. Law No. 27 of 2022 concerning Personal Data Protection
   Based on Article 1 Paragraph (2) of the Personal Data Protection Law, personal data protection is a comprehensive effort to protect personal data in the personal data processing chain to guarantee the constitutional rights of personal data subjects. The standards of personal data protected by the PDP Law are important for understanding the criteria for personal data that must be protected under the PDP Law in order to have proper data protection and meet the criteria for personal data under the PDP Law. Article 1 Paragraph 1 of the PDP Law explains that personal data is data of a person or individual that is identified or can be identified individually or combined with other information, either directly or indirectly through electronic or non-electronic systems.
b. Law No. 19 of 2016 concerning Electronic Information and Transactions
   Personal data protection under this law includes data protection from unauthorized use, data protection by electronic system providers, and data protection from unlawful access and interference. In other words, any use of information involving a person's personal data through electronic media or systems must obtain the consent of the individual concerned.
c. Regulation of the Minister of Communication and Information Technology No. 20 of 2016 concerning Personal Data Protection
   In this regulation, personal data refers to the personal information of a particular individual that is processed, maintained, and kept accurate and confidential. Furthermore, Article 5 paragraph (4) explains, "other preventive measures to avoid failures in protecting the Personal Data they manage must be carried out by every Electronic System Organizer, at least in the form of activities.
d. Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions
   In this GR, the term 'Electronic System Provider' refers to individuals, state entities, business entities, and communities that provide Electronic Systems. They are responsible for the provision, operation, and/or management of electronic systems, either individually or collectively, for the benefit of electronic system users, both for their own benefit and for the benefit of other parties.

Various legal protections for the privacy rights of Indonesian citizens have been regulated in various laws and regulations in Indonesia. Personal data protection has been recognized as a type of human rights and accommodated in international legal instruments. In this case, personal data protection is an intersection of the right to information and the right to privacy through a long evolutionary process since the recognition of human rights through the Universal Declaration of Human Rights (UDHR) 1948. Article 12 of the UDHR specifically regulates the protection of a person's right to privacy, namely, "No one shall be subject to arbitrary interference with his privacy, family, or correspondence, nor to attack upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.[93]

The term "privacy" in this article is an umbrella term associated with the protection of one's family, residence, and correspondence, as well as one's honor and reputation. Substantively, the UDHR provides very broad protections for the right to privacy. First, physical privacy, which aims to protect privacy related to a person's residence.

[92] Moh Bagas Fadhli Dzil Ikrom and Badrut Tamam, "Perlindungan Hukum Hak Privasi Warga Negara terhadap Kebocoran Data Pribadi di Indonesia," *Jurnal Konstitusi* 3, no. 2 (December 2024).
[93] Asbjørn Eide, *The Universal Declaration of Human Rights: A Commentary* (Oslo: Scandinavian University Press, 1992), 188.

Second, decisional privacy, which aims to protect a person's privacy so they can determine their own life, including their family's. Third, dignity, which aims to protect privacy related to a person's self-worth, including their good name and reputation. Fourth, informational privacy, which aims to protect a person's privacy so they can access and store their personal data.[94]

The formulation of Article 28G paragraph (1) of the 1945 Constitution has the same nuance of protection as the formulation of Article 12 UDHR which was then adopted into Article 17 ICCPR which has been ratified in Law No. 12 of 2005 concerning ratification which explicitly provides guarantees for the right to privacy. In Constitutional Court Decision No. 50/PUU-VI/2008, the Constitutional Court provided a translation of Article 12 UDHR and Article 17 ICCPR, namely the word privacy is translated as *urusan pribadi/masalah pribadi*, that:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.[95]

However, despite a clear legal framework, the implementation of this law often faces obstacles in addressing the increasingly widespread problem of data leaks. The leaked information includes National Identification Numbers (NIK), Family Cards (KK), full names, and other personal data. This incident highlights the vulnerability of citizens' personal data in electronic systems used by the government and state institutions. Although the leakages have been reported and received public attention, the government's efforts to handle such cases are still considered to be insufficiently effective.[96]

3.2.2. Surveillance Culture: Shifting the Paradigm from Protecting Citizens to Suspicion of Citizens

In addition to violations of freedom of expression and opinion, one of the rights most vulnerable to erosion due to the militarization of technology is the right to privacy. Increasingly sophisticated and complex cybercrime modus operandi has the potential to be carried out through the misuse of technology in the field of data and information management, one of which is the breach and theft of personal data. In the modern context, violations of the right to privacy no longer occur solely through physical wiretapping or conventional surveillance, but also through the use of digital devices, data, and intelligence-based security systems with a militaristic orientation for surveillance purposes.

Angus Willoughby (2017) uses the term biometric technology as a technology that raises human rights concerns.[97] This is because biometric technology is often associated with privacy violations, especially when applied in the context of surveillance, because this technology allows administrators to identify someone, or verify someone's identity, at a later date.[98]

---

[94] Eide, *The Universal Declaration of Human Rights*, 188.; Elfian Fauzi and Nabila Alif Radika Shandy, "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi," *LEX Renaissance* 7, no. 3 (July 7, 2022): 445–461.

[95] Aditiya Putra, Apakah Hak atas Privasi Termasuk HAM?" *Hukumonline.com*, February 3, 2025, https://www.hukumonline.com/klinik/a/apakah-hak-atas-privasi-masuk-ham-lt4f5f850ec2388/.

[96] Moh Bagas Fadhli Dzil Ikrom and Badrut Tamam, "Perlindungan Hukum Hak Privasi Warga Negara terhadap Kebocoran Data Pribadi di Indonesia," *Jurnal Konstitusi* 3, no. 2 (December 2024).

[97] Angus Willoughby, "Biometric Surveillance and the Right to Privacy," October 5, 2017, https://technologyandsociety.org/biometric-surveillance-and-the-right-to-privacy/.

[98] In his writing, Willoughby explains that Biometrics refers to the process of recording, measuring, and analyzing various human physiological features. The scope of features that can be covered by biometrics is "all-encompassing, and includes appearance, behavior, and cognitive state." Certain physiological traits are permanent, unique, and universal. These traits are known as "biometric characteristics." These characteristics are usually measured by a series of sensors and stored in a database as "templates." According to the goals of biometric system managers, templates allow managers to identify a person, or verify a person's identity, at a later date. Willoughby, "Biometric Surveillance and the Right to Privacy."

Figure 7. Illustration of Biometric Authentication, Identification, and Verification



Source: recfaces.com

While widely claimed to contribute to successful defense strengthening, for example in the United States, militaries and intelligence agencies are increasingly employing biometric technology in intelligence, surveillance, and reconnaissance (ISR) activities and have reported other successes arising from the use of biometrics, such as intelligence gathering on improvised explosive devices and counter-piracy operations.[99] In this context, biometrics is part of a broader strategy that combines identification through biometric technology with other ISR methods to identify, track, or profile individuals. This combination of methods can expand surveillance capabilities over individuals and increase the risk of privacy violations. Depending on the nature and implementation of a particular biometric technology, its use may violate a country's international human rights obligations. More specifically, it remains uncertain how such technology interacts with the human right to privacy.[100]

David Lyon (2018), a sociologist from Queen's University, explains that from 9/11 to the Snowden data leaks, surveillance has dominated the global government agenda and even headlines. Surveillance has transformed, not only being carried out on a person's existence, but also extending to what individuals do in their daily lives. This condition, according to David Lyon, is part of a culture of surveillance.

A widespread culture of surveillance can be seen in China. From camera-filled streets to apps requiring biometric identification, the use of facial recognition has flourished in the country. This situation has sparked public concern. A survey conducted by the Beijing News Think Tank found

[99] Willoughby, "Biometric Surveillance and the Right to Privacy."
[100] Willoughby, "Biometric Surveillance and the Right to Privacy."

that out of 1,515 Chinese respondents, 87.46 percent opposed the use of facial recognition technology in commercial areas.[101]

Figure 8. Portrait of the Controversy over Biometric Technology in China against Human Rights



Source: South China Morning Post

This culture has normalized surveillance, making us submit to it and believe we have nothing to hide. David Lyon explains that when the state has the ability to collect and analyze data on a massive scale, citizens lose autonomy and agency over their personal data. This shifts the relationship between the state and society into a hierarchical one based on control, not trust.[102]

Furthermore, militarization of technology widens the gap between security and freedom, shifting the paradigm of citizen protection to one of suspicion. In a democratic context, this contradicts the principle of the rule of law, which places individuals as subjects, not objects, of state power. As a result, public trust in security institutions can be eroded, and the state's legitimacy in carrying out its security functions is questioned.

In the Indonesian context, securing public privacy is even more challenging due to the porous data security systems of various state institutions, resulting in personal data leaks. For example, the BPJS Kesehatan data leak in May 2021, followed by the sale of participant data on Raid Forums for 0.15 Bitcoin. Then there was the data leak of 2.3 million Indonesian citizens from the General Elections Commission (KPU) in May 2020. The leaked data included names, addresses, ID numbers, dates of birth, and other information.

Furthermore, SAFEnet's (2020) findings indicate that digital media is also used as a means of repression against civil society, including through various forms of digital attacks. Based on monitoring throughout 2020, there were 147 incidents of digital attacks. The peak of digital attacks occurred in October 2020, with 41 incidents. The numerous incidents in October were

[101] South China Morning Post, "Facial Recognition Is Used in China for Everything from Refuse Collection to Toilet Paper Dispensers and Its Citizens Are Growing Increasingly Alarmed, Survey Shows," 2021, https://www.scmp.com/tech/innovation/article/3119281/facial-recognition-used-china-everything-refuse-collection-toilet.
[102] David Lyon, *The Culture of Surveillance: Watching as a Way of Life* (Cambridge: Polity Press, 2018), https://www.perlego.com/book/1536337/the-culture-of-surveillance-watching-as-a-way-of-life-pdf.

related to Indonesia's political situation. In October 2020, the Indonesian government passed the Job Creation Law, also known as the Omnibus Law. The enactment of the Job Creation Law sparked opposition among civil society, even becoming a trending topic on Twitter. This widespread opposition was accompanied by a surge in digital attacks against students, activists, and civil society organizations.[103]

In general, digital attacks fall into two categories. First, there are hard attacks, which typically involve specific tools and techniques to attack targets or even take over the victim's assets. Examples of attacks that fall into this category include hacking, eavesdropping, and distributed denial of service (DDoS) attacks. Not everyone can carry out these hard attacks, as they require specific technology and skills.[104]

Second, soft attacks. Attacks using this method are more aimed at psychologically intimidating the victim (psywar) or destroying their credibility in the public eye. Therefore, these soft attacks must be carried out openly through social media by the perpetrators, whether anonymous or real. Examples of attacks in this category include the unauthorized dissemination of personal identities (doxing), account impersonation (impersonation), and trolling through comments or posts.[105]

Meanwhile, various cases of militarization of technology that threaten citizens' privacy in Myanmar can serve as a lesson. The Myanmar military junta is installing Chinese-made cameras with facial recognition capabilities in numerous cities across the country, claiming to maintain civil peace. However, human rights activists familiar with the projects raise serious concerns that the devices could be used to crack down on activists and resistance groups, both of which were designated as terrorists by the junta after the coup. The military and police could use them to track their movements, establish connections between activists, and identify safe houses and other gathering places.[106]

[103] Southeast Asia Freedom of Expression Network (SAFEnet), *Laporan Situasi Hak-hak Digital Indonesia 2020: Represi Digital di Tengah Pandemi* (Denpasar: Southeast Asia Freedom of Expression Network (SAFEnet), 2021).
[104] SAFEnet, *Laporan Situasi Hak-hak Digital Indonesia* 2020.
[105] SAFEnet, *Laporan Situasi Hak-hak Digital Indonesia* 2020.
[106] VOA Indonesia, "Perketat Pengawasan, Junta Myanmar Pasang CCTV Canggih China di Lebih Banyak Kota," July 7, 2022, https://www.voaindonesia.com/a/perketat-pengawasan-junta-myanmar-pasang-cctv-canggih-china-di-lebih-banyak-kota-/6653414.html.

Figure 9. Myanmar Junta Government Installs Chinese-Made Cameras



Source: Reuters

Human Rights Watch asserts that the military junta's access to a new public camera system equipped with facial recognition and license plate recognition technology poses a serious threat to citizens' fundamental rights. While billed as a Safe City initiative, since December 2020 the government has deployed 335 surveillance cameras in eight townships in the capital, Naypyidaw. The technology actually allows the government to monitor the habits and movements of community members, thus potentially causing detrimental side effects that threaten people's privacy.[107]

Another issue relates to the lack of clarity regarding which officials or parties will be granted access to the data. In Myanmar, facial recognition and license plate recognition technology were rolled out without adequate public consultation or transparency. Consequently, there is no clarity regarding the steps authorities plan to mitigate the potential impact of the technology's use on human rights, particularly the right to privacy.[108]

Furthermore, it is important to understand that this technology can also be used to isolate individuals in a discriminatory or arbitrary manner, including based on their ethnicity or religion. The situation in China also offers a lesson, as facial recognition and license plate recognition have been used for mass surveillance purposes. In the Xinjiang region, the Chinese government uses a variety of technologies, including facial recognition, surveillance cameras, and big data programs, to monitor and track Uighurs and other citizens. Anyone marked as "problematic" based on unclear criteria can be sent to political education camps and subjected to political indoctrination.[109]

---

[107] Human Rights Watch, "Myanmar: Facial Recognition System Threatens Rights: Camera Surveillance, Mass Data Collection Bolsters Abusive Junta," March 12, 2021, https://www.hrw.org/news/2021/03/12/myanmar-facial-recognition-system-threatens-rights.

[108] Human Rights Watch, "Myanmar: Facial Recognition System Threatens Rights."

[109] Human Rights Watch, "Myanmar: Facial Recognition System Threatens Rights."

4. What are the Regulations and Accountability Regarding the Militarization of Technology?

The integration of digital technologies—such as surveillance systems, cyber weapons, artificial intelligence, autonomous weapons systems, and big data analytics—into military structures is not only accelerating operational transformation but also expanding the potential impact on human rights. The pace of adoption of these technologies is also often outpacing regulatory development, creating governance gaps that pose serious challenges for regulation, accountability, and transparency.

In the Indonesian context, accountability and transparency in the field of national defense have been long-standing issues with no clear developments to date. Arifianto (2005) in his study *The Military Budget Management System in Indonesia: A Review of Control Aspects, Transparency and Public Accountability*, shows that the budget and financial management system of the Department of Defense-TNI has inherent weaknesses that affect the effectiveness of the system, namely a budget authorization and funding system that is too rigid, bureaucratic, and inflexible; the absence of task limitations that are able to regulate internal control; and a financial accountability system lacking in transparency and accountability, with risks of irregularities.[110]

In the context of regulations, both public and state, a dilemma exists between the need to maintain confidentiality and democratic governance that places accountability and transparency as primary principles. Even within the national legal framework, Law No. 14 of 2008 concerning Public Information Disclosure, Article 17 letter c explains that certain information is exempt from public disclosure, such as information related to national defense and security, namely:

1. Information about strategy, intelligence, operations, tactics and techniques related to the implementation of the national defense and security system, including the planning, implementation and termination or evaluation stages in relation to threats from within and outside the country.
2. Documents containing strategies, intelligence, operations, techniques and tactics related to the implementation of the national defense and security system, including the planning, implementation and termination or evaluation stages.
3. The number, composition, disposition or allocation of forces and capabilities in the implementation of the national defense and security system and its development plans.
4. Images and data on the situation and condition of military bases and/or installations; and 5. Data on estimates of the military and defense capabilities of other countries are limited to all actions and/or indications of the country that could endanger the sovereignty of the Republic of Indonesia and/or data related to military cooperation with other countries agreed in the agreement as confidential or top secret.

The provisions of Article 17 letter c of Law No. 14 of 2008 concerning Public Information Disclosure (KIP), which provide exceptions for information related to national defense and security, are in principle intended to protect strategic confidentiality that could threaten national security if disclosed to the public. However, in the practice of defense sector governance in Indonesia, these exceptions are often used as normative justification to excessively limit public access to information that is not actually categorized as sensitive,

[110] Yuniar Arifianto, Military Budget Management System in Indonesia: Review of Control, Transparency and Public Accountability Aspects (Depok: Faculty of Economics and Business, University of Indonesia, 2005), https://lib.ui.ac.id/detail?id=83595&lokasi=lokal.

such as budget allocations, procurement processes, and defense program performance evaluations.[111]

This has serious implications on democratic governance, as the defense sector is a domain traditionally considered to be highly sensitive and confidential. In fact, many meetings between Commission I of the House of Representatives (DPR) and the Indonesian National Armed Forces (TNI) are held behind closed doors under this pretext, including those discussing the issue of procurement of weapons systems.[112] Paradoxically, when the government emphasizes state secrets, the weapons systems procurement process will ultimately also be publicized through various mass media and institutions that sell the weapons to Indonesia, including information on prices, specifications, and year of production.[113]

The high level of secrecy within the defense sector, particularly in developing countries like Indonesia, structurally contributes to the increasingly uncontrolled militarization of technology. The secrecy practiced by the military—through information restrictions, minimal reporting mechanisms, and the absence of transparency in technology procurement, testing, and use—creates a policy space that civilian authorities or the public find hard to monitor. When states widely deploy digital surveillance systems or cyber tools under the guise of security without robust transparency mechanisms, it can lead to an erosion of civil liberties and privacy.

Given the complexity of the issue and its potential impact on democratic decline, regulations regarding the militarization of technology are urgently needed. Such regulations are needed to ensure that the use of defense technology is based on the principles of legality, necessity, and proportionality, and falls under effective oversight and accountability mechanisms. With an adequate regulatory framework, states can maintain a balance between national security interests and the protection of citizens' rights, while preventing the normalization of unaccountable surveillance practices that could potentially undermine democracy.

4.1. How can budget use be accounted for?

The first regulation relates to budget transparency. Within a democratic framework, defense budget transparency serves not only as a managerial instrument but also as a political accountability mechanism. Budget transparency allows parliament and the public to assess whether defense spending priorities align with national security interests and constitutional values, including the protection of human rights.

However, enormous efforts are required to achieve this ideal state. Available data on defense budgets and budgeting processes are very limited and often unreliable. Public and media pressure on the government to disclose information is also generally limited. Leaders often withhold defense-related information, arguing that too much information poses a threat to national security. This rhetoric is now widespread in several countries, such as China, where the authorities do not even publish the approved state budget.[114]

---

[111] This situation was evident, among other things, during the third presidential debate in the 2024 election, which focused on defense and security. Prabowo Subianto, one of the presidential candidates, repeatedly cited state secrets as a pretext for discussing weapons systems budgets and other defense issues.

[112] Detik.com, "Rapat Komisi I DPR, Panglima TNI Tertutup Saat Bahas Alutsista," October 22, 2024, https://news.detik.com/berita/d-5560339/rapat-komisi-i-dpr-panglima-tni-tertutup-saat-bahas-alutsista; Fachri Audhia Hafiez, "Rapat Bahas Anggaran Alutsista Menhan dengan Komisi I DPR Digelar Tertutup," MetroTVNews.com, June 12, 2024, https://www.metrotvnews.com/read/bD2C1Qj6-rapat-bahas-anggaran-alutsista-menhan-dengan-komisi-i-dpr-digelar-tertutup.

[113] Vitorio Mantalean and Ardito Ramadhan, "Imparsial: Pengadaan Alutsista Rawan Korupsi dengan Dalih Rahasia Pertahanan," *Kompas.com*, December 10, 2024.

[114] Mariya Gorbanova and Leah Wawro, *The Transparency of National Defense Budgets: An Initial Review* (London: Transparency International UK, 2011).

Another factor is the lack of human resource capacity and understanding, which hinders many governments' ability to publish defense budget information. This situation is further complicated by the limited universally accepted definition of military spending, which makes it difficult to determine the precise composition of defense budget items to be publicly disclosed.[115]

Accountability and transparency of the budget used in the provision of military technology need to be seen as part of the Constitutional rights of citizens, as regulated in Article 28F of the 1945 Constitution of the Republic of Indonesia, namely:

> "Everyone has the right to communicate and obtain information to develop their personality and social environment, and has the right to seek, obtain, possess, store, process, and convey information using all available channels."

This article emphasizes that information disclosure is not merely an administrative policy, but rather a constitutional right inherent in citizens and an important prerequisite for accountability, transparency, and civil control in a democratic state.

Furthermore, it is important to understand that defense and security are public services provided by the state and funded by citizens' taxes. Therefore, the relationship between the state and citizens in this sector is contractual within a democratic framework: public funds collected through taxes demand public accountability. Therefore, citizens' right to know how their tax money is spent cannot be overridden under the pretext of national security. However, it is also understood that certain operational and tactical information must be protected for the sake of national security.

However, accountability should not override the confidentiality of information that needs to be protected. Defense budget transparency does not necessarily mean making all information public, but also includes other mechanisms that allow for ongoing oversight and accountability. There are at least two ways to achieve this. First, information on defense spending and investments in alternative public services, focusing on how defense spending levels impact other development priorities where state intervention is needed. For example, Eisenhower noted in 1953 that the cost of one bomber aircraft is equal to the cost of building 30 schools, two power plants, or two hospitals.[116]

Second, to increase transparency in the defense budget while reducing the risk of disclosure of highly sensitive security-related information, South Korea has established three categories of defense budget information, each based on its level of confidentiality. Category A presents budget items for discussion to the entire National Assembly in aggregate form. Category B presents budget items to designated members of the National Assembly Committee of National Defense in more detailed and separate form. Category C presents items further and presents them only to the Committee of National Defense. Previously, legislators were only given total figures for debate.[117]

Furthermore, South Korea's journey in strengthening transparency and accountability in its defense budget can serve as a reference. In addition to categorizing defense budget information, South Korea also has four strategies for increasing domestic defense transparency: [118]

1. The Ministry of National Defense (MND) provides information to the public through its website homepage. The MND homepage introduces defense policy to the public through

[115] Gorbanova and Wawro, *The Transparency of National Defense Budgets*.
[116] Gorbanova and Wawro, *The Transparency of National Defense Budgets*.
[117] Gorbanova, Mariya, and Leah Wawro. *The Transparency of National Defense Budgets: An Initial Review*. London: Transparency International UK, 2011.
[118] Beomchul Shin, *The Republic of Korea's Perspective on Defense Transparency*, Policy Brief No. 2011-1 (Northeast Asia Defense Transparency Project, University of California Institute on Global Conflict and Cooperation, October 2011).

the posting of the MND organizational chart, defense news, and key policy papers. In particular, the MND continues to inform the public about its support for civilians and seeks public input through the "Participation Plaza," a question-and-answer section to address public concerns about defense. In addition, the MND provides defense news to 3,000 civilian experts and retired officers through Public Customer Relationship Management (PCRM).

2. The MND holds regular press conferences twice daily to explain current defense issues. Continuous media monitoring is the best way to improve defense transparency. Since South Korea faces North Korea militarily, most of its defense information is classified as state secrets. However, improving the quality of defense transparency can be done by enabling media monitoring. Spokespeople answer questions submitted in advance, explain issues to the public, and hold question-and-answer sessions. Through these briefings, the MND strives to ensure the public receives timely defense-related news. In addition to these briefings, the MND publishes the Korea Defense Daily, which provides defense news to active and retired military personnel and civilian experts.
3. Third, the defense white paper, published every two years, is the most important publication providing a comprehensive explanation of defense policy to the public. In the year prior to its publication, the MND seeks expert input from Korean think tanks to improve the quality of subsequent white papers. Through these efforts, the MND ensures that the material in the defense white paper is well-received by the public.
4. Fourth, the National Assembly plays a crucial role in promoting defense transparency through its annual inspection and budget deliberations. The inspections, which take place immediately after September 10 each year, last 20 days. During the inspection period, the National Assembly can review various defense policy issues, and the Ministry of Defense must provide materials requested by the National Assembly. The National Assembly can also launch an independent investigation if serious violations in defense management are found.

South Korea's strategy of ensuring accountability and transparency in defense issues can serve as a reference for Indonesia. Defense budget discussions in Indonesia remain subject to a regime of excessive secrecy, both by the President, as the holder of government power and commander-in-chief, and by the House of Representatives (DPR), the representative body supposed to carry out budget oversight. The most frequently used excuse to justify limited public access is "state secrets."

For example, when Commission I of the Indonesian House of Representatives held a working meeting with the Ministry of Defense (Kemhan), the TNI Commander, the Army Chief of Staff, the Air Force Chief of Staff, and the Navy Chief of Staff on June 12, 2024, which discussed the evaluation of the 2024 budget and the discussion of the 2025 Draft State Budget. Because the meeting discussed the budget of the Ministry of Defense and the TNI related to weapons systems, it was finally decided to be closed.[119] A similar thing was also done in 2025, precisely on July 9, 2025, when the Minister of Defense (Menhan) Sjafrie Sjamsoeddin together with the TNI Commander General Agus Subiyanto held a closed meeting with Commission I of the Indonesian House of Representatives. The meeting was held to discuss the work plan and budget for 2026.[120]

The secrecy surrounding defense budget discussions in Indonesia has ultimately reached a problematic point. Meetings between the government and the House of Representatives (DPR) are held behind closed doors under the pretext of state secrets, yet the public is "shocked" by

[119] Dwi Rahmawati, "Bahas Anggaran Kemhan 2025, Rapat Komisi I DPR Digelar Tertutup," *detikNews*, June 12, 2024, https://news.detik.com/berita/d-7386957/bahas-anggaran-kemhan-2025-rapat-komisi-i-dpr-digelar-tertutup.

[120] Adrial Akbar, "Rapat Tertutup di DPR, Menhan-Panglima TNI Usul Tambah Anggaran Rp 184 T," *detikNews*, July 9, 2025,https://news.detik.com/berita/d-8003834/rapat-tertutup-di-dpr-menhan-panglima-tni-usul-tambah-anggaran-rp-184-t.

the news that the defense budget has been significantly increased. This pattern reveals a serious paradox in democratic governance: strategic fiscal decisions are taken without an adequate public deliberation process, but the financial impact is borne by the wider community.

One example is seen in the results of a closed meeting in July 2025, when the Ministry of Defense proposed an additional budget of IDR 184 trillion.[121] In a situation like this, claims of state secrecy no longer function as security protection, but rather as a shield to close the decision-making process from democratic oversight.[122]

Ultimately, the public can see and understand that, in practice, in Indonesia, the concept of state secrecy in the defense budget is not treated as a narrowly tailored exception, but rather as a general justification for closing almost the entire budgeting cycle—from planning and deliberation to evaluation. The House of Representatives (DPR), which constitutionally has budgetary oversight authority, tends to reproduce the executive's logic rather than correct it. Defense budget discussions are often held behind closed doors. Meanwhile, in South Korea, the National Assembly plays a crucial role in promoting defense transparency through its annual budget inspections and deliberations.

Furthermore, South Korea's transparency and accountability in the defense sector is also demonstrated through the publication of the Defense White Paper every two years, demonstrating public accountability for the direction of the country's defense policy. This practice demonstrates that even a country with a high level of military threat still views transparency as an integral part of national security, not a threat to it.

In contrast, Indonesia lacks a tradition of regularly publishing defense white papers that are easily accessible to the public. As a result, the public struggles to understand the link between the threats faced, the chosen defense strategy, and the budget increases requested by the country. The Indonesian Defense White Paper was last published in 2015 by the Indonesian Ministry of Defense. However, no updated edition has been officially released to the public since then.

South Korea's defense budget transparency and accountability are notable for its long history and strong political will. When Kim Young Sam, the first civilian president in more than three decades, took office in 1993, his administration purged factions within the military, investigated corruption in defense procurement, and promoted transparency in defense spending. The National Assembly and the independent press acted and reported on incidents of corruption related to the military—without exception. Through these processes, defense transparency has been greatly enhanced from a domestic perspective.[123]

During the Lee Myung-Bak administration (2008-2013), South Korea's defense transparency was continuously enhanced. The administration also sought to enhance defense transparency by declaring "defense for the people" as the foundation of its policy. Under this slogan, the government sought to provide more information to the public and garner public support. In providing defense-related information to meet public demand, the Korean government also increased cooperation with the international community.[124]

In the domestic context, accurate and transparent defense budgeting is a crucial prerequisite for ensuring that state resources are allocated effectively across the various functions carried out

[121] Akbar, "Rapat Tertutup di DPR."
[122] Ironically, some of the recent justifications for defense budget increases include improving personnel welfare. This rationale raises a fundamental question: since when have issues of soldier welfare—related to salaries, allowances, and basic services—been categorized as state secrets? No operational or intelligence aspects are compromised when the public knows the direction of state apparatus welfare policies.
[123] Shin, *The Republic of Korea's Perspective on Defense Transparency*.
[124] Shin, *The Republic of Korea's Perspective on Defense Transparency*.

within the defense and security sector. Without clear and transparent budget planning, resource distribution risks being unequal, not based on strategic needs, and likely driven by short-term bureaucratic interests. Beyond these domestic reasons, a transparent defense budgeting process can provide regional and international benefits. Excessive secrecy can lead to higher levels of uncertainty and suspicion at the regional and global levels.[125]

4.2. Have Laws Been Violated in the Procurement of Military Equipment?

Military procurement is one of the areas of public policy most vulnerable to legal violations due to the large budgets involved, high levels of secrecy, and strong power relations between state actors and technology providers. In this context, legal violations—such as irregularities in procurement procedures, conflicts of interest, budget overruns, or procurement without a clear strategic basis—not only result in financial losses for the state but also have the potential to undermine defense governance and democratic accountability. When procurement processes proceed without strict legal compliance, the space for public and parliamentary oversight becomes increasingly limited, increasing the risk of abuse of power.

One of the highlights of the procurement of tools related to the militarization of technology can be seen in the report by Amnesty International – in collaboration with its media partners, Haaretz, Inside Story, Tempo, the WAV research collective, and Woz – titled *A Web of Surveillance – Unraveling a murky network of spyware exports to Indonesia*. The report shows that between 2017 and 2023, there was a systematic pattern in the procurement and use of highly intrusive surveillance technology by a number of entities in Indonesia,[126] both from the state sector and those related to national security interests.[127]

A variety of advanced spy software and surveillance technologies have reportedly been imported and distributed, reflecting the growing reliance on digital instruments for intelligence and security control purposes. Among the technologies mentioned are Pegasus—the notorious spy software developed by the Israel-based NSO Group—and Predator, a high-performance spyware platform developed by the international consortium Intellexa. Furthermore, the report also revealed the existence of the Cyrus cyberinfiltration system, a product of Israeli surveillance technology vendor Saito Tech (also known as Candiru), designed to covertly infiltrate and monitor digital devices.[128]

The sale and transfer of spy software and surveillance technology is made possible through an opaque ecosystem of vendors, brokers, and surveillance resellers with complex ownership structures.[129] Meanwhile, Indonesia has Law No. 16 of 2012 concerning the Defense Industry which should serve as the framework and policy basis for various defense-security equipment procurements in Indonesia.[130] Through the provisions of Article 2, it can be understood that priority is the main principle in the Implementation of the Defense Industry, as well as accountability is also one of the principles. This provision can be an illustration that the Implementation of the Defense Industry is not merely protected by the principle of confidentiality, making it difficult to touch its accountability.

---

[125] Gorbanova and Wawro, *The Transparency of National Defense Budgets*.

[126] ASEAN Parliamentarians for Human Rights (APHR), "Indonesia Must Halt the Import and Use of Highly Invasive Spyware from Israel and Elsewhere, Southeast Asian MPs Say," May 6, 2024, https://aseanmp.org/publications/post/indonesia-must-halt-the-import-and-use-of-highly-invasive-spyware-from-israel-and-elsewhere-southeast-asian-mps-say/.

[127] In its report, Amnesty International explains that these entities include the Indonesian National Police (Kepolisian Negara Republik Indonesia) and the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara).

[128] APHR, "Indonesia Must Halt the Import and Use of Highly Invasive Spyware."

[129] Amnesty International, "Unraveling a Murky Network of Spyware Exports."

[130] Article 1 point 2 of the Law explains that Defense and Security Equipment is all equipment to support national defense as well as public security and order.

The said Law, through Article 43 also regulates the procurement of defense and security equipment from abroad or foreign products. However, such procurement cannot be carried out immediately, but has certain mechanisms and conditions. In the context of the mechanism, in paragraph (3) of Article 43 it is stated that procurement must first be through a proposal to the Defense Industry Policy Committee (KKIP), which is chaired by the President, to use foreign products with procurement through a direct intergovernmental process or to manufacturers. Even in the context of national strategic interests, the DPR provides consideration in the procurement of certain Defense and Security Equipment products in accordance with the foreign policy implemented by the Government in Article 43 paragraph (4).

Meanwhile, the procurement of defense and security products from abroad, as regulated in Article 43 paragraph (5), has requirements that must be met, including:

a. Defense and Security Equipment has not been or cannot be made domestically;
b. Involving Defense Industry Participation;
c. Technology transfer obligations;
d. Guarantee that there is no potential for embargo, political conditionality and obstacles to the use of Defense and Security Equipment in efforts to maintain state sovereignty, the territorial integrity of the Unitary State of the Republic of Indonesia, and the safety of the entire nation from threats and disturbances to the integrity of the nation and state;
e. There is a trade-off, local content and/or offset of at least 85% (eighty-five percent);
f. Local content and/or offset as referred to in letter e is at least 35% (thirty five percent) with an increase of 10% (ten percent) every 5 (five) years; and
g. The offset will be implemented no later than 18 (eighteen) months from the date this Law is enacted.

In more detail, the provisions for the procurement of military equipment are regulated through the Minister of Defense Regulation No. 17 of 2014 concerning the Implementation of the Procurement of Main Weapons systems within the Ministry of Defense and the Indonesian National Armed Forces. In its definition, Article 1 number 2 explains that the procurement of a weapons systems is an activity to obtain a weapons systems whose stages are preceded by planning needs until the receipt of a weapons systems that functions according to its designation.

Then Article 5 paragraph (1) emphasizes that the procurement of TNI weapons systems must use domestic production. However, the provisions in paragraph (2) open up foreign production space, that if the TNI weapons systems as referred to in paragraph (1) cannot be fulfilled by the Domestic Defense Industry, procurement of foreign products can be carried out through a direct process between governments or to manufacturers. The fundamental thing that should be considered is the principles of procurement. Through the provisions of Article 8, it is stated that there are transparent principles in budget management and accountability.

However, there is also a principle of ensuring confidentiality that can be a principal justification for the lack of transparency in this procurement. Furthermore, the provisions regarding the procurement evaluation team, as stipulated in Article 21, also need to be taken seriously. First, the “existing” authority in the form of providing advice in the implementation of the procurement. Even the procurement evaluation team is not required to sign an Integrity Pact. This condition needs to be highlighted, because the Integrity Pact is not merely an administrative procedure, but a normative foundation that strengthens public trust, increases the legitimacy of evaluation results, and ensures that the evaluation functions as a credible accountability mechanism in organizational governance.

Then, through the Minister of Defense Regulation No. 17 of 2014, it is understood that there are stages in the implementation of the procurement of TNI weapons systems which are structured with five stages, namely:

1. The first stage, namely the pre-preparation stage.
   This stage includes identifying weapons systems needs based on defense doctrine, the TNI's strategic plan, and threat analysis. At this stage, weapons systems needs are formulated conceptually and strategically, including determining initial specifications and their alignment with the state budget. This stage is crucial because it serves as the foundation for procurement legitimacy; errors or manipulation at this stage have the potential to result in procurement that is irrelevant, excessive, or fraught with non-defense interests.
2. The second stage, namely the preparation stage
   This stage involves the preparation of more technical procurement documents, including final specifications, financing schemes, and procurement plans. This stage also includes technical and administrative feasibility studies and the preparation of procurement mechanisms in accordance with laws and regulations. In the context of the militarization of technology, the preparation stage should also provide a space to incorporate long-term risk considerations, including technological dependency, data security, and potential impacts on human rights, although these aspects are not explicitly regulated in the Ministry of Defense Regulation.
3. The third stage, namely the stage of selecting the TNI weapons systems provider
   This stage is the most sensitive in terms of integrity and potential legal violations. It encompasses the selection, evaluation, and determination of defense goods and services providers, both domestic and international. Given the strategic and often classified nature of weapons systems, this stage is often conducted using special mechanisms. However, without adequate oversight, this phase is vulnerable to corruption, conflicts of interest, and a disregard for the principle of value for money.
4. The fourth stage, namely the contract preparation and activation stage
   This stage is when the legal relationship between the state and the weapons systems supplier is formalized. The contract includes the scope of work, the parties' obligations, the timeframe, and dispute resolution mechanisms. In the procurement of modern military technology, the contract should also address aspects of technology transfer, data protection, and liability for system failures. Weaknesses in this stage can have long-term consequences, especially if the contract does not adequately protect the state's interests or creates strategic dependence on foreign parties.
5. The fifth stage, namely the implementation and submission stage of work results
   This stage encompasses the production, delivery, testing, and handover of weapons systems to the Indonesian National Armed Forces (TNI). It is also a crucial step to ensure that the received weapons systems meets specifications, functions properly, and is operationally ready. From an accountability perspective, this stage requires a strong monitoring and evaluation mechanism, because failure or deviation in this phase can have direct implications on defense effectiveness and waste the state budget.

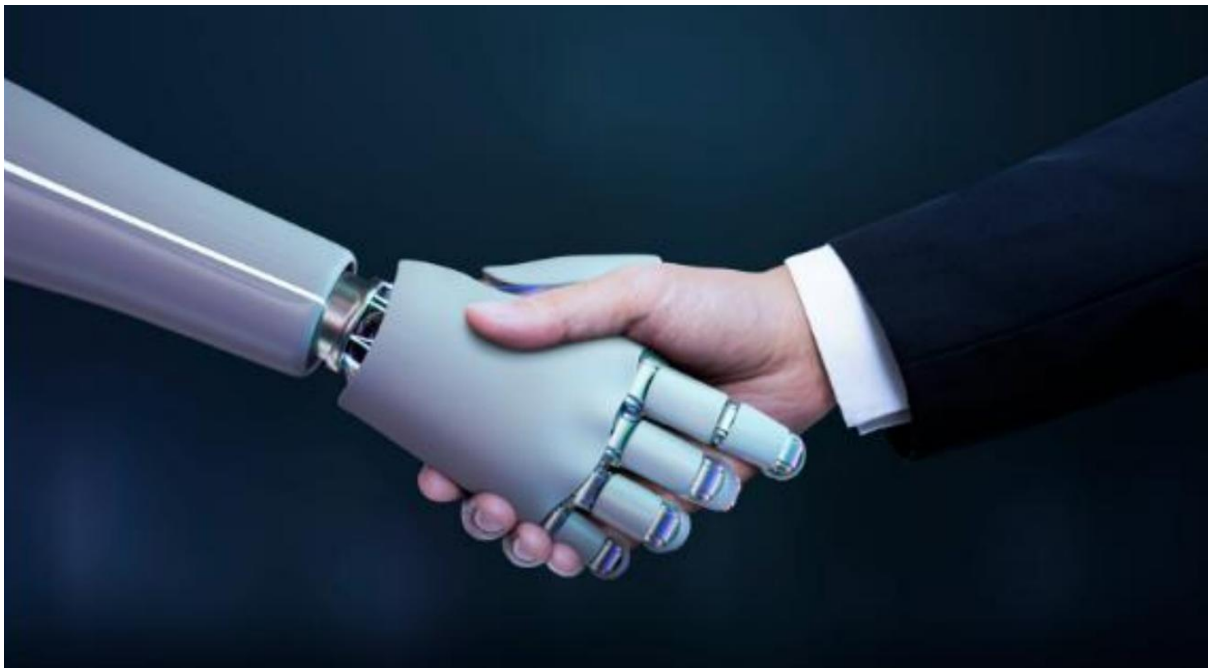
Overall, Defense Ministerial Regulation No. 17 of 2014 demonstrates that the procurement of weapons systems for the Indonesian National Armed Forces (TNI) has been designed through systematic and multi-layered stages. However, in the contemporary context of the militarization of technology—particularly digital, cyber, and surveillance technologies—this regulation still tends to be oriented towards procedural and administrative aspects, without explicitly incorporating the dimensions of human rights protection, public transparency, and social risk assessment. Therefore, strengthening derivative regulations and integrating human rights principles and democratic accountability are important agendas to ensure that weapons

systems procurement is not only procedurally valid, but also legitimate from a legal and ethical standpoint.

4.3. How can the accountability model be frameworked?

The rapid development of digital technologies—such as artificial intelligence (AI), surveillance systems, cyber technology, drones (UAVs), and digital intelligence tools—has transformed Indonesia's defense and security landscape. On the one hand, these technologies are seen as crucial for addressing non-traditional and complex threats. However, on the other hand, the militarization of technology without mechanisms for accountability, transparency, and human rights protection has the potential to lead to serious violations of the right to privacy, freedom of expression, and the principle of civilian control over the military.

Figure 10. Technology Settings to Stay Ethical



Source: https://widya.ai/

A framework for accountability is needed to ensure that the militarization of technology in Indonesia remains within the framework of a democratic state based on the rule of law and respect for human rights, emphasizing the importance of civilian oversight, budget accountability, and risk-based regulation. As a basic regulation, the militarization of technology must ensure compliance with various legal provisions that guarantee citizens' rights, such as the 1945 Constitution of the Republic of Indonesia, Law No. 39 of 1999 concerning Human Rights, Law No. 27 of 2022 concerning Personal Data Protection, and various international instruments related to International Humanitarian Law and international human rights.

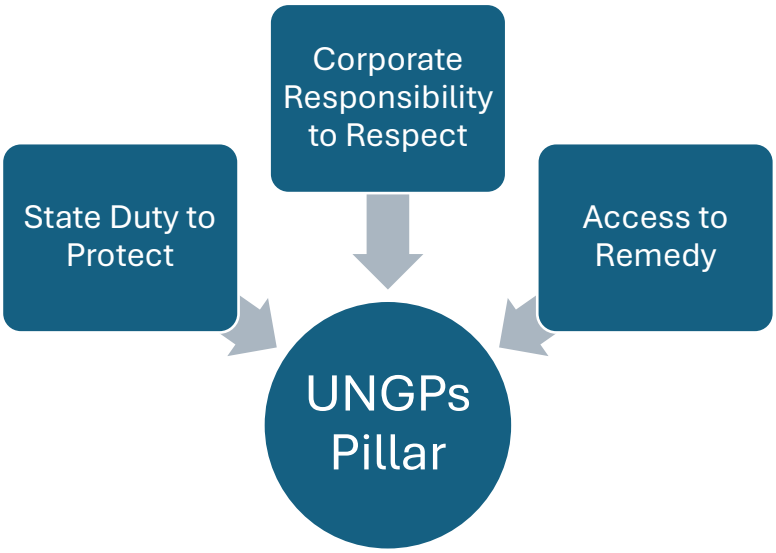
This compliance is strengthened and/or also realized through systems, such as in the aspects of supervision and accountability: (1) strengthening the supervisory function by legislative institutions, specifically substantive supervision, not just formalities; (2) ensuring multi-layered supervision by involving institutions such as the National Commission on Human Rights and the Indonesian Ombudsman, as well as preparing preventive mechanisms to anticipate violations and responsive public complaint mechanisms after violations occur; (3) categorizing, like South Korea, information that can be accessed by the public, both in budget documents and technology procurement reports.

Regulatory aspects and complaint mechanisms also need to be emphasized, such as (1) as part of the construction of a state of law and ensuring legal certainty, the procurement and use of technology must have an explicit legal basis, not just internal military policy; (2) permission to use certain technologies (spyware, AI surveillance) must be given before use, not after violations occur; and (3) citizens must have access to sue for misuse of technology (e.g. illegal surveillance).

One fundamental point in designing such regulations can be drawn from Arifianto's (2005) research, which asserts that there is no need for special treatment for the overall management of the military budget (Dephan-TNI). Special treatment should be limited to contingency and confidential matters, such as urgent or sudden military operations, by improving the internal control system and a more transparent and accountable financial accountability system in order to realize good governance in the management of state finances.[131]

Various previous explanations show that in the context of the militarization of technology, states are increasingly forming partnerships with private actors, whether as technology providers, system developers, or support operators. This pattern creates an expansion of actors involved in practices that have the potential to limit or violate human rights, particularly the rights to privacy, freedom of expression, and protection from arbitrary surveillance. In such situations, the application of human rights due diligence (HRDD), as emphasized in the United Nations Guiding Principles on Business and Human Rights (UNGPs), becomes important.

Compliance with the UNGPs can pressure companies to adopt the 3 (three) main pillars of the UNGPs, namely:



Adopting human rights due diligence in military-private partnerships enables the identification, prevention, and mitigation of human rights risks from the planning and procurement stages to the use of military technology. Thus, HRDD serves not only as an ethical instrument but also as a concrete mechanism to ensure that the militarization of technology remains within a framework of democratic accountability, the rule of law, and respect for human rights, even when implemented through complex relationships between the state and the private sector.

The UNGP principles also need to be developed to incorporate a gender-based perspective. For example, accountability mechanisms must ensure the meaningful participation of women and

[131] Arifianto, *Sistem Pengelolaan Anggaran Belanja Militer di Indonesia*.

gender-based civil society organizations in the monitoring, evaluation, and formulation of digital security policies. Limited transparency, currently justified in the name of national defense and security, must be balanced with sufficient disclosure of information to assess human rights risks, including the risk of gender-based violence and discrimination. Furthermore, access to complaint and remedy mechanisms must be designed to be safe, inclusive, and responsive to the experiences of female victims, whether in the administrative, judicial, or non-judicial spheres.

In addition, the basic principles of International Humanitarian Law (IHL) are a reference for limiting methods and means in warfare, which is referred to in regulating military technology that intersects with human rights. There are four basic principles in question, namely: [132]

1. Distinction: there must be a clear distinction between armed forces and civilians, and between objects that may be lawfully attacked and objects that are protected from attack.
2. Military necessity: parties to an armed conflict may only use force to the extent and type not prohibited by the law of armed conflict, which is necessary to achieve the legitimate aim of the conflict, namely the complete or partial defeat of the enemy as quickly as possible with the minimum expenditure of resources.
3. Humanity: humanity prohibits the infliction of suffering, injury or damage that is not actually necessary for the achievement of legitimate military objectives.
4. Proportionality: the losses resulting from a military action must not be too great compared to the expected military advantage.

International humanitarian law affirms the principle of distinction, which requires parties to a conflict to distinguish civilian objects from legitimate military targets. This requires multiple verification procedures before digital targeting, as well as a human-in-the-loop obligation, meaning humans still decide on attacks. Furthermore, the principle of necessity limits the use of force or technology that is not necessary to achieve legitimate military objectives.

Strengthening regulations on the militarization of technology could also include adopting NATO's AI governance Principles of Responsible Use (PRUs) for military applications. These six principles, updated in 2024, aim to ensure that AI is used safely and ethically within the bounds of international law and democratic values:[133]

1. Lawfulness: The use of AI must comply with national and international laws, including international humanitarian law.
2. Responsibility and Accountability: Human responsibility must be maintained, and accountability cannot be transferred to machines.
3. Explainability and Traceability: AI must be understandable and transparent, with appropriate review and validation mechanisms.
4. Reliability: AI is intended for specific use cases, with safety and security tested throughout its lifecycle.
5. Governability: AI design must allow for human interaction, detect unintended consequences, and have the capacity to deactivate.
6. Bias Mitigation: Steps should be taken to minimize unwanted bias in AI development, use, and training data.

[132] Foreign & Commonwealth Office and Foreign, Commonwealth & Development Office, "The UK and International Humanitarian Law," GOV.UK, July 24, 2018, updated April 4, 2024, https://www.gov.uk/government/publications/international-humanitarian-law-and-the-uk-government/uk-and-international-humanitarian-law-2018.

[133] NATO, *Summary of NATO's Revised Artificial Intelligence (AI) Strategy*, 10 July 2024, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy.

These regulations and restrictions on the militarization of technology are in line with the EU Artificial Intelligence Act, Article 5: Prohibited AI Practices, which prohibits certain uses of artificial intelligence. These include AI systems that manipulate human decisions or exploit their vulnerabilities, systems that evaluate or classify people based on their social behavior or personal characteristics, and systems that predict a person's risk of committing a crime.[134]

The law also prohibits AI systems that extract facial images from the internet or CCTV footage, infer emotions in workplaces or educational institutions, and categorize people based on their biometric data. However, some exceptions are made for law enforcement purposes, such as locating missing persons or preventing terrorist attacks.[135]

The European Union's experience with the EU Artificial Intelligence Act, particularly Article 5 on Prohibited AI Practices, provides important normative standards regarding the limits of high-risk technology use. These rules emphasize that technological innovation must not undermine human dignity, privacy, and democratic principles. By prohibiting practices such as behavioral manipulation through AI, predicting criminal risk based on personal characteristics, the widespread use of biometric identification from CCTV or online images, and emotional inference in workplaces or education, the EU demonstrates that technological boundaries can be firmly set without compromising collective security goals.

In the Indonesian context, these principles provide an important foundation that the militarization of technology must be guided by universal human rights norms, the rule of law, and democratic civilian control. Military use of technology should not be expanded without limits or evaluation, especially when it involves mass surveillance, biometric data collection, or predictive analytics that could potentially criminalize certain groups. While exceptions for law enforcement purposes—such as searching for missing persons or preventing acts of terrorism—are reasonable, such practices must remain subject to strict oversight mechanisms, judicial authorization, and measurable human rights evaluations.

Therefore, Indonesia needs to develop a regulatory framework that aligns with international standards, by adopting the basic principles of the EU AI Act: prohibition of harmful AI, risk-based governance, and democratic accountability.

Such regulations should include substantive limitations on the use of high-risk technologies, independent evaluation mechanisms, and civilian oversight of the procurement and implementation of military technology. For a legally enforceable accountability model, the legislative level may be the primary option.

4.4. Examining Regulations Related to the Militarization of Technology in Indonesia

In the context of the militarization of technology, the problems can be categorized into five aspects, including: (1) The absence of specific regulations governing the use of digital military technology, especially surveillance and AI technology; (2) The pretext of defense secrecy is often used to limit budget transparency and public information (UU KIP Article 17); (3) Limited and asymmetric parliamentary oversight, especially in the procurement of intelligence tools and cyber systems; (4) Minimal assessment of human rights impacts before the procurement and use of defense technology; and (5) The risk of normalizing mass surveillance, especially in cyberspace and against civilians.

Although there are no specific regulations, in the context of the regulatory framework, Indonesia actually has several relevant legal instruments to ensure the democratization of technology,

[134] "Article 5: Prohibited AI Practices https://artificialintelligenceact.eu/article/5/rticle 5: accessed December 2, 2025
[135] "Article 5: Prohibited AI Practices."

although they have not been specifically designed to regulate the impact of military technology on human rights and democratic governance.

In principle, these provisions are contained in the Constitution, specifically Article 28D, which provides for the right to recognition, guarantees, protection, fair legal certainty, and equal treatment before the law. Furthermore, Article 28G regulates the right to protection of self, family, honor, dignity, property, and a sense of security. These principles were later reinforced through Law No. 39 of 1999 concerning Human Rights.

Various international human rights instruments that have been ratified by Indonesia can also be used as reinforcement in regulating the militarization of this technology, including:

1. International Covenant on Civil and Political Rights (ICCPR). This instrument is the primary basis for limiting the use of surveillance technology by states. The ICCPR guarantees: the right to privacy, freedom of expression, and freedom of assembly and association. Any restrictions on these rights, including through military technology or digital intelligence, must meet the principles of legality, necessity, and proportionality. The ICCPR is highly relevant for assessing the use of military surveillance in civilian spaces and domestic security operations. This instrument has been ratified through Law No. 12 of 2005 concerning the Ratification of the International Covenant on Civil and Political Rights.
2. International Covenant on Economic, Social, and Cultural Rights (ICESCR). Although it does not directly regulate surveillance, the ICESCR is important in the context of state budget priorities. The militarization of technology absorbing significant budgets has the potential of reducing the fulfillment of the rights to education, health, and social welfare. This instrument strengthens the argument that military technology spending must be subject to the principles of maximum available resources and fiscal accountability. This instrument was ratified through Law No. 11 of 2005 concerning the Ratification of the International Covenant on Economic, Social, and Cultural Rights.
3. Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT). The CAT instrument is relevant when surveillance technology is used for profiling, targeting individuals, or intelligence operations that result in arbitrary detention. This is because the use of technology to support repressive practices can give rise to state responsibility, including if the technology facilitates torture or inhumane treatment. This instrument has been ratified through Law No. 5 of 1998 concerning the ratification of the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment.
4. Convention on the Rights of the Child (CRC). The CRC instrument can strengthen restrictions on the use of surveillance technology on children, students, and educational spaces. Biometric-based surveillance technology, digital monitoring, or the collection of child data by state officials must comply with the principles of the best interests of the child and the protection of child privacy. This instrument has been ratified through Presidential Decree (Keppres) No. 36 of 1990 which ratified the “Convention on the Rights of the Child” or the UN Convention on the Rights of the Child.
5. Convention on the Elimination of All Forms of Discrimination against Women (CEDAW). The CEDAW instrument is relevant in the context of the risk of gendered surveillance, when security technology can be used in a discriminatory manner against women, activists, or vulnerable groups. This instrument strengthens the obligation of states to ensure that military technology does not deepen inequality and discrimination. This instrument was ratified through Law No. 7 of 1984 concerning the Ratification of the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW).

The strengthening of human rights principles and constitutional guarantees is evident in Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), which focuses on protecting citizens' rights, particularly personal data. Its considerations include two key points:

1. Protection of personal data is a human right which is part of personal self-protection, so it is necessary to provide a legal basis to provide security for personal data, based on the 1945 Constitution of the Republic of Indonesia
2. Personal data protection is aimed at guaranteeing citizens' rights to personal protection and raising public awareness as well as ensuring recognition and respect for the importance of personal data protection;

The Personal Data Protection Law provides an important normative foundation for limiting the use of data-based technologies, including surveillance technology, biometrics, and artificial intelligence systems commonly used in the defense and intelligence sectors. This is because it affirms that personal data controllers,[136] as stipulated in Article 38, are obliged to protect personal data from unauthorized processing.

In addition, Law No. 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and its amendments (UU ITE) in the context of strengthening the regulation of the militarization of technology, also contains a number of provisions that implicitly protect digital civil rights, so that they can function as a supporting domestic instrument (supporting legal framework) in controlling the impact of the militarization of technology, especially in cyberspace. For example, Article 30 of the ITE Law regulates the prohibition of unauthorized access to electronic systems belonging to others, Article 32 of the ITE Law prohibits the destruction, alteration, or transfer of electronic data without authorization.[137]

The various regulations above emphasize the state's obligation to protect the fundamental rights of individuals from all forms of abuse of power, including those mediated by technological developments. In the context of the militarization of technology and the use of surveillance systems by the government through state apparatus, the Constitution and the Human Rights Law provide a normative basis that the rights to privacy, freedom of opinion, expression, and security are inherent rights of every individual and cannot be arbitrarily reduced. The state, including military and security institutions, is bound by the principle of respecting, protecting, and fulfilling human rights in all policies and actions, regardless of the pretext of national security.

5. The Use of Dual-use Technology in the Context of Indonesian Military Modernization and Its Impact on Human Rights

Context and Relevance

Military spending is often justified on grounds of deterrence and national security. However, evidence shows that increased military spending does not always lead to greater peace or stability. Instead, it often exacerbates geopolitical tensions, fuels arms races, and increases the risk of conflict, particularly when associated with weak governance, rising inequality, and systemic mistrust. Rising military spending is currently diverting resources essential for

[136] In the Law, Article 1 number 4 defines Personal Data Controller as any person, public body, and international organization that acts individually or jointly in determining the purpose and exercising control over the processing of Personal Data.

[137] However, there are also notes regarding the ITE Law, such as the potential for expanding state authority in technology-based regulation, supervision and law enforcement, and the fact that it does not explicitly limit the actions of state officials, especially when linked to national security reasons.

social investment, poverty reduction, education, health, environmental protection, and infrastructure – undermining progress on nearly all of the Sustainable Development Goals.[138]

Meanwhile, global military spending has been rising at a record pace for a decade in response to the deteriorating global security environment.[139] According to new data published by the Stockholm International Peace Research Institute (SIPRI), global military spending is expected to reach $2,887 billion in 2025, a 2.9 percent increase in real terms compared to 2024. Military spending declines in the United States but increases by 14 percent in Europe and by 8.1 percent in Asia and Oceania. The three largest military spenders, the United States, China, and Russia, spend a combined $1,480 billion, or 51 percent of the global total. Global military spending is expected to rise again in 2025 as countries respond to another year of war, uncertainty, and geopolitical turmoil with large-scale weaponization.[140] Governments and companies around the world are racing to establish dominance and engage technology users in a technology race. The technology race has redefined the battlefield and blurred the lines between civilian and military infrastructure. This dramatic shift affects every aspect of every individual's life and reshapes the future of humanity and radically changes political and investment priorities.[141] The government is rapidly militarizing society with a political strategy of increasing military spending that has implications for weakening civil rights protections and reducing social protection programs. The era of globalization is marked by governments increasingly relying on the private sector to provide public services, through public-private partnerships.[142]

Large digital platforms like Facebook, Amazon, Microsoft, Alphabet (Google), and Apple, often referred to as Big Tech, now dominate the global economy. Big Tech's market capitalization has surpassed the gross domestic product of large economies such as Germany or Japan. Big Tech also controls a significant portion of global research and development and patents related to cutting-edge technologies, such as artificial intelligence. These facts reflect an unprecedented concentration of techno-economic power, with significant implications for income distribution, access to knowledge and innovation, the fragmentation and precarization of labor, and rising geopolitical tensions. The core power of Big Tech companies is manifested in their control of knowledge, infrastructure, such as data centers, submarine cables, and dual-use technologies, such as cloud computing, artificial intelligence, and new satellite navigation and communication systems, which are crucial for both civilian and military purposes.[143]

At the same time, over the past decade, the center of the American military-industrial complex has slowly shifted from Washington, D.C., to Silicon Valley. While the bulk of the Pentagon's $886 billion budget is spent on conventional weapons systems,[144] a new political economy is emerging

---

[138] United Nations. Secretary-General, *The Security We Need: Rebalancing Military Spending for a Sustainable and Peaceful Future: Report of the Secretary-General on the Impact of the Global Increase in Military Expenditure on the Achievement of the Sustainable Development Goals Requested by Action13(c) of the Pact for the Future* (2025), https://digitallibrary.un.org/record/4088022/files/SG_Report_TheSecurityWeNeed.pdf.

[139] Nan Tian and Xiao Liang, "Rebalancing Military Spending Towards Achieving Sustainable Development," *SIPRI Research Policy Paper* (Stockholm: Stockholm International Peace Research Institute [SIPRI], November 2025), https://doi.org/10.55163/ZCIE5196.

[140] SIPRI, "Global Military Spending Rise Continues."

[141] Privacy International, "Challenging the Militarisation of Tech," https://privacyinternational.org/campaigns/militarisation-of-tech.

[142] Privacy International, "What Is Militarization of Tech?" September 12, 2025, https://privacyinternational.org/long-read/5668/what-militarisation-tech.

[143] Andrea Coveri, Claudio Cozza, and Dario Guarascio, "Big Tech and the US Digital-Military-Industrial Complex," *Intereconomics* 60, no. 2 (2025): 81–87, https://doi.org/10.2478/ie-2025-0017.

[144] The budget is channeled to established defense giants such as Lockheed Martin, RTX, Northrop Grumman, General Dynamics, Boeing, and BAE Systems. See Roberto J. González, *How Big Tech and Silicon Valley Are Transforming the Military-Industrial Complex* (Costs of War, Watson Institute for International and Public Affairs, Brown University), April 17, 2024), https://costsofwar.watson.brown.edu/paper/how-big-tech-and-silicon-valley-are-transforming-military-industrial-complex.

driven by large technology companies, venture capitalists, and private equity firms that support the military industry. As U.S. Department of Defense officials seek to adopt artificial intelligence-powered systems and secure cloud computing services, the Department has awarded major contracts worth billions of dollars to Microsoft, Amazon, Google, and Oracle. At the same time, the Pentagon has increased funding for smaller defense technology startups that seek to disrupt existing markets and move fast and break things.[145]

Over the past two years, global events have further fueled the Pentagon's demand for Silicon Valley technology, including the deployment of drones and AI-powered weapons systems in Ukraine and Gaza, as well as concerns about a global AI arms race against China. The prospect of Russian cyberwarfare and disinformation campaigns has also motivated Defense Department officials to invest heavily in new digital technologies. This has prompted U.S. Department of Defense officials to outline plans to develop a vast fleet of autonomous aerial, maritime, and ground drones for transportation, surveillance, and combat; and to acquire commercial cloud computing capabilities for data sharing, data storage, and seamless connectivity. These new digital technologies will strengthen U.S. cyber defense systems and utilize artificial intelligence for training and simulated combat exercises.[146]

This situation places Big Tech companies as key players in the clash between two digital-military-industrial complexes competing for global hegemony. This competition contributes to a blurring of the boundaries between states and corporations compared to the situation in the second half of the 20th century with the rise of transnational corporations. In this regard, Elon Musk's role in the Donald Trump administration and the loyalty shown by other Big Tech CEOs during the inauguration ceremony support the hypothesis of a convergence of strategic interests in military-technological development.[147]

Today, the military and intelligence apparatus cannot function without Big Tech. These companies control digital tools, including cloud systems and artificial intelligence algorithms for image and voice recognition, behavioral prediction, and military targeting, which are essential for spying on enemies and allies and anticipating their movements on the battlefield. These companies play a crucial role in the military-related innovation ecosystem, helping mobilize research and development efforts from startups and facilitating the transfer of technologies designed for civilian domains to the military. Furthermore, media platforms run by Big Tech, such as the social media platform X, owned by Elon Musk, support political consensus-building and influence public opinion, both at home and abroad.[148]

At the same time in recent years venture capital spending on defense technology has reached a record high by 2025, with defense-tech start-ups being backed by venture capital in the United States and Europe. Some forecasts calculate venture capital support for defense tech start-ups to reach a total of $7.7 billion between January and October 2025, more than double the total in 2024. Overall, private defense investment in 2025 is expected to exceed $48 billion, driven by large funding rounds for companies in the artificial intelligence and autonomous drones. This growing interest is largely a result of promises of high government spending on defense and growing interest in the uses of artificial intelligence on the battlefield.[149]

In addition to the steady rise in global military spending over the past decade, the reach of military technology has also expanded, with the lines between instruments of war and peace becoming

[145] González, *How Big Tech and Silicon Valley Are Transforming the Military-Industrial Complex*.
[146] González, *How Big Tech and Silicon Valley Are Transforming the Military-Industrial Complex*.
[147] Coveri, Cozza, and Guarascio, "Big Tech and the US Digital-Military-Industrial Complex."
[148] Coveri, Cozza, and Guarascio, "Big Tech and the US Digital-Military-Industrial Complex."
[149] Katja Bego, "How a Surge in Defense and Dual-Use Technology Investment Could Reconfigure the Global AI Race," *Chatham House*, April 28, 2026, https://www.chathamhouse.org/2026/04/how-surge-defence-and-dual-use-technology-investment-could-reconfigure-global-ai-race/02.

increasingly blurred. The UK, Europe, and the US are leveraging technologies developed on the battlefield to monitor citizens and keep an eye on refugees at their borders. Arms giants are becoming key technology providers to police, border agencies, and other public bodies.[150] Today, dual-use technologies span a wide range of industries and technological fields, including artificial intelligence, advanced materials, nanotechnology, cybersecurity tools, satellite technology, biotechnology, quantum, aerospace, and drones. Dual-use technologies are not just a defense and commercial strategy; they are also a business strategy for innovative companies. Companies developing and commercializing dual-use technologies must manage two often distinct customer and value chains. While there are benefits to having multiple customers from both government and commercial buyers.[151]

Russia's full-scale invasion of Ukraine in 2022 has been a major factor behind the resurgence of interest in dual-use and defense technologies. The war in Ukraine has not only triggered a significant increase in global military spending but also demonstrated the utility of commercially available technological innovations on the modern battlefield. While large platforms and traditional weapons systems will not lose their importance in war, Ukraine has revolutionized the extensive and innovative use of inexpensive, disposable drones, enabled by dual-use systems like Starlink.[152]

In the Indonesian context, modernizing weapons and strengthening the defense industry have long been priorities for the Indonesian government, particularly the current administration led by President Prabowo Subianto. The achievement of the weapons modernization ambition can be traced to the trend of increasing military spending in 2025.[153] Furthermore, the budget increase is evident in the 2027 Draft State Budget (RAPBN) for defense, where the government has allocated Rp 329.5 trillion. This figure is an increase of approximately Rp 30 trillion compared to the outlook for Fiscal Year 2026, when the defense function was estimated at Rp 299.1 trillion.[154]

The significant budget increase marks the return of militarization under President Prabowo Subianto. According to Norman Joshua, the militarization under President Prabowo Subianto will be seen in two ways: (1) an increase in the military budget and; (2) a broader role for the military in non-security matters. The increasing role of the military and police, both active and retired, in non-military matters has tended to begin during the administration of President Joko Widodo. At the same time, under Prabowo's presidency, there has been a systematic effort to restore the military's dual function, which includes defense-security duties as well as socio-political duties.[155] Drew Holland Kinney calls this situation praetorianism, a situation in which the military

---

[150] Corporate Watch, "What's Driving the Militarization of Tech—and What We Can Do about It," https://corporatewatch.org/whats-driving-the-militarization-of-tech-and-what-we-can-do-about-it/.

[151] James W. Hinton, Dual-Use Technologies in the Age of Intangibles, *Policy Brief* No. 215 (Waterloo, ON: Center for International Governance Innovation [CIGI], November 3, 2025), https://www.cigionline.org/publications/dual-use-technologies-in-the-age-of-intangibles/.

[152] Bego, "How a Surge in Defense and Dual-Use Technology Investment."

[153] Although the 2025 budget allocation has increased compared to the previous year, doubts still surround efforts to accelerate weapons modernization along with the expansion of the Indonesian military organization (TNI) and the defense budget which is still below 1% of GDP. See, Adhi Priamarizki and Edna Caroline, Prabowo's Defence Challenge: Making "Triple Helix" Work, *IDSS Paper* IP26067 (Singapore: S. Rajaratnam School of International Studies, Nanyang Technological University, May 21, 2026), https://rsis.edu.sg/rsis-publication/idss/ip26067-prabowos-defence-challenge-making-triple-helix-work/. The outlook for defense functions until the end of 2025 is estimated at IDR 245.2 trillion or 147.7% of the 2025 State Budget ceiling. See, Dovana Hasiana, "Anggaran Pertahanan 2025 Dipatok Naik 47% Jadi Rp245 Triliun," Bloomberg Technoz, July 6, 2025, https://www.bloombergtechnoz.com/detail-news/76302/anggaran-pertahanan-2025-dipatok-naik-47-jadi-rp245-triliun.

[154] CNN Indonesia, "Pemerintah Siapkan Rp329,5 Triliun untuk Pertahanan di RAPBN 2027," August 19, 2026, https://www.cnnindonesia.com/nasional/20260819113956-20-1393907/pemerintah-siapkan-rp3295-triliun-untuk-pertahanan-di-rapbn-2027.

[155] Michael Breger, "The Legacies of Militarization: Norman Joshua Writes a Social and Cultural History of Indonesian Authoritarianism," FSI, Stanford University, April 17, 2024, https://fsi.stanford.edu/news/legacies-militarization-norman-joshua-writes-social-cultural-history-indonesian.

plays a dominant role in political structures and institutions, tends to frequently intervene to influence politics and constitutional change, and can dominate the political system or vice versa.[156] Anthony Forster reminds us that the study of civil-military relations is not enough to only discuss the threat of military intervention in domestic politics. The study also needs to pay attention to the role of actors outside conventional armed forces, such as paramilitary groups and intelligence agencies, which are referred to as grey forces.[157]

The expansion of the TNI's authority to the cyber realm, which is standardized through the framework of military operations other than war through Law Number 3 of 2025, actually negates the characteristics of the cyber realm itself. Cyberspace introduces a decentralized mode of coordination, reconfiguring authority, sovereignty, and governance, and challenging norms of civilian control.[158] Militarism in social media is legalized by this law. Based on the provisions of Article 7 paragraph 2 letter b point 15, the TNI is given attributive authority to assist in efforts to overcome cyber threats. The expansion of the TNI's role in overcoming cyber threats could open up space for the state to target parties who wish to criticize the government. Further impact, this authority could threaten citizens' freedom of expression on social media.[159]

The expansion of authority was then strengthened through Presidential Regulation (Perpres) Number 85 of 2025 revising Presidential Regulation Number 151 of 2024 concerning the Ministry of Defense. Based on this regulation, the Indonesian Ministry of Defense established a new nomenclature, namely the Defense Intelligence Information and Communication Agency, which has the authority to manage defense intelligence information and communication.[160] This renewal of authority will add institutions that will tend to strengthen state surveillance in the digital space, but instead have the potential to create serious risks for civil liberties and the fundamental rights of citizens. On the other hand, the characteristics of cyberspace should change the organization and culture of the TNI, including adapting strategies to reconfigure the dynamics of civil-military relations in the cyber realm.

Military authority also has the potential to expand after a long period of stagnation in space research and development in Indonesia. Since taking office in October 2024, President Prabowo has repeatedly emphasized the importance of developing the space sector in his speeches. Then, in January 2025, the Secretary-General of the Indonesian Space Association, Aryo P S Djojohadikusumo, announced that Indonesia would participate in global space research, with the National Research and Innovation Agency (BRIN) as the primary agency coordinating cooperation with various universities. Furthermore, Indonesia also plans to upgrade its aging space infrastructure.

Erna Sri Adiningsih, director of the Indonesian Space Agency (INASA), which was formed under BRIN,[161] said Indonesia's space plans focus on improving space technology, remote data

---

[156] Valerij Shpak, "Indirect Praetorianism: The Case of Turkey's Military," *Scientific Journal of the Military University of Land Forces* 54, no. 4(206) (2022): 624–638, https://doi.org/10.5604/01.3001.0016.0757.

[157] Francesco F. Milan, Three Generations of Studies in Civil-Military Relations: A Primer, *Revista Científica General José María Córdova*, vol. 24, no. 53, 2026

[158] Isabella Neumann, "It Is Complicated: Cyber into the Civil–Military Relationship," *Journal of Cybersecurity* 12, no. 1 (2026): 1–12, https://doi.org/10.1093/cybsec/tyag012.

[159] Dewa Ayu Diah Angendari, "Militerisme di Media Sosial: Bagaimana UU TNI Mengancam Kebebasan Sipil di Dunia Siber," *The Conversation*, https://theconversation.com/militerisme-di-media-sosial-bagaimana-uu-tni-mengancam-kebebasan-sipil-di-dunia-siber-254065.

[160] Kompas.com, "Kemenhan Bentuk Badan Baru, Diminta Pastikan Tidak Ada Tumpang Tindih," August 8, 2025, https://nasional.kompas.com/read/2025/08/08/20124741/kemenhan-bentuk-badan-barudiminta-pastikan-tidak-ada-tumpang-tindih.

[161] As part of its mandate, BRIN provides satellite-based remote sensing technology assistance to the government, giving the government a central role in space-related applications for economic development, law enforcement, and national defense. See, University World News, "Indonesia Ramps Up Space R&D to Reduce Foreign Reliance," November 25, 2025, https://www.universityworldnews.com/post.php?story=20251125121827251.

analysis and processing, and space security through international cooperation.[162] On June 24, 2025, the Indonesian Defense University (Unhan RI) launched the RIDU-Sat 1 nanosatellite. The launch was carried out using SpaceX's Falcon 9 Transporter 14 Rideshare rocket.[163] The commitment to utilizing outer space was further strengthened when the Indonesian National Air Operations Command officially established a dedicated Space Unit in January 2026. The Air Force Chief of Staff previously stated publicly that the future of Indonesia's defense lies in space, and control of this domain will be key to national sovereignty in the modern era. However, the Space Unit still lacks a clear legal basis to support Indonesia's domestic and international obligations bound by treaties on space law.[164]

Meanwhile, based on data from the Indonesia National Procurement Portal (Inaproc), provider package 63689327 is listed in the form of a social media monitoring system with a budget ceiling of IDR 49,235,461,000. The social media monitoring system procurement package worth IDR 49.2 billion by the Ministry of Defense in the 2026 budget year. The method of selecting goods and services providers is through direct appointment with the work unit (satker) of the Indonesian Army Headquarters. The contract implementation schedule begins in February 2026 and ends in February 2026.[165] Although later, the Indonesian Army stated that the social media monitoring procurement contract had not been carried out with any party, including for the social media monitoring system procurement package worth IDR 49.2 billion.[166]

At the same time, Indonesia currently lacks laws specifically regulating the legitimate use of spyware and surveillance technology. This situation is exacerbated by Indonesia's political culture, which has created a burgeoning spyware ecosystem, making it increasingly difficult to detect cases of illegal misuse against civilians. Furthermore, this situation risks creating impunity designed to perpetuate human rights violations.[167] On another front, Indonesia's export control measures are at best out of step with global norms. Indonesia is not a member of any multilateral export control regime, nor does it have a list of dual-use goods subject to control. Jakarta's opposition to strategic trade controls stems from concerns that dual-use goods controls developed by developed countries discriminate against developing countries and could hinder Indonesia's access to dual-use technology.[168] Spyware has often been considered a vital tool for law enforcement and intelligence operations. However, numerous examples of countries using it in ways that violate human rights and undermine democracy and the rule of law.[169]

The Amnesty International report, titled "Building an Imaginary Enemy," shows the manifestation of the TNI's authority to handle military operations other than war. Amnesty International's report mentions the alleged involvement of Indonesian authorities, including the military, in using

---

[162] University World News, "Indonesia Ramps Up Space R&D."
[163] Ministry of Defense of the Republic of Indonesia, "Unhan RI Sukses Luncurkan Satelit Nano Indonesia, RIDU-Sat 1," June 25, 2025, https://www.kemhan.go.id/2025/06/25/unhan-ri-sukses-luncurkan-satelit-nano-indonesia-ridu-sat-1.html.
[164] Taufik Rachmat Nugraha and Bich Tran, Bridging the Legal and Strategic Mismatch in the Indonesian Air Force's Space Unit, *IDSS Paper* IP26100 (Singapore: S. Rajaratnam School of International Studies, Nanyang Technological University, 27 August 2026), https://rsis.edu.sg/rsis-publication/idss/ip26100-bridging-the-legal-and-strategic-mismatch-in-the-indonesian-air-forces-space-unit/.
[165] Kompas.id, "Publik Pertanyakan Anggaran Rp 49,2 Miliar untuk Monitoring Medsos TNI AD," April 29, 2026, https://www.kompas.id/artikel/anggaran-rp-492-miliar-untuk-monitoring-medsos-tni-ad-dipertanyakan-publik.
[166] Kompas.id, "Kadispenad: Kontrak Monitoring Medsos Rp 49,2 Miliar Tidak Pernah Dilaksanakan," April 30, 2026, https://www.kompas.id/artikel/kadispenad-kontrak-monitoring-medsos-rp-492-miliar-tidak-pernah-dilaksanakan.
[167] Amnesty International, *A Web of Surveillance*.
[168] Matthew P. Goodman, Matthew Reynolds, and Julianne Fittipaldi, "Economic Security in Emerging Markets: A Look at India, Vietnam, and Indonesia," *CSIS Brief* (Washington, DC: Center for Strategic and International Studies(CSIS), May 17, 2022), https://www.csis.org/analysis/economic-security-emerging-markets-look-india-vietnam-and-indonesia.
[169] Lena Riecke, "Unmasking the Term 'Dual Use' in EU Spyware Export Control," *European Journal of International Law* 34, no. 3 (2023): 697–720, https://doi.org/10.1093/ejil/chad039.

online disinformation to target journalists, activists, academics, and demonstrators in retaliation for their activism and legitimate expression.[170] The case of Andrie Yunus, deputy coordinator of the Commission for Missing Persons and Victims of Violence (KontraS), shows a pattern of linkage between coordinated online campaigns and physical attacks. Andrie Yunus had been the target of a coordinated online campaign that described him as a "foreign agent" after several months of peaceful protests against the revision of the TNI Law:[171]

> This incident did not happen out of the blue; it was long-planned and preceded by an organized online disinformation campaign involving multiple actors – designed to undermine his credibility and delegitimize his career as a human rights defender using the label of a "foreign agent" – and a sustained offline effort to intimidate him.

The UN High Commissioner for Human Rights, Michelle Bachelet stated.[172]

> Serious concerns about the dangers of authorities using surveillance tools from various sources that are supposed to enhance public security to hack the phones and computers of people carrying out legitimate journalistic activities, monitoring human rights, or expressing political dissent or opposition.
>
> Governments must immediately stop using their own surveillance technology in ways that violate human rights, and must take concrete action to protect against such privacy violations by regulating the distribution, use, and export of surveillance technology created by others.

A similar view was also expressed by Gina Romero, Special Rapporteur on freedom of peaceful assembly and of association, who stated:[173]

> Narratives about foreign agents often label and target civil society and protesters. These labels often base these accusations on the type of funding they receive. Civil society organizations that receive foreign funding are explicitly targeted and attacked with harassment and stigmatization campaigns. This labeling is accompanied by excessive surveillance and potential restrictions on civil society's access to resources. The stigmatization of foreign agents further undermines the public trust necessary for civil society to do its work.
>
> These narratives have become a widespread instrument of stigmatization aimed at delegitimizing activists and associations, and are supported and reinforced by the widespread adoption of so-called "foreign agent" laws. This narrative has resulted in criminalization and, in some countries, mass disbandment of civil society organizations designated as foreign agents.
>
> This is further fueled by smear campaigns against civil society organizations receiving foreign funding, including the publication by authorities of lists of such organizations. These lists have also been published on social media or by media outlets using negative,

---

[170] Amnesty International, "Indonesia: Military Silences Dissent with Disinformation Campaigns Branding Activists and Journalists 'Foreign Agents'," May 19, 2026, https://www.amnesty.org/en/latest/news/2026/05/indonesia-military-silences-dissent-disinformation-campaigns-branding-activists-journalists-foreign-agents/.

[171] Amnesty International, Membangun Musuh Khayalan: Misinformasi, Disinformasi dan Tuduhan "Antek Asing" di Bawah Presiden Prabowo di Indonesia, ASA21/0931/2026 (May 19, 2026), https://www.amnesty.org/en/documents/asa21/0931/2026/id/.

[172] Office of the United Nations High Commissioner for Human Rights (OHCHR), "Use of Spyware to Surveillance Journalists and Human Rights Defenders: Statement by UN High Commissioner for Human Rights Michelle Bachelet," 19 July 2021, OHCHR.

[173] Gina Romero, Protecting the Right to Freedom of Peaceful Assembly and of Association from Stigmatization, Report of the Special Rapporteur on the Right to Freedom of Peaceful Assembly and of Association, UN Doc.A/79/263 (United Nations, July 31, 2024), https://digitallibrary.un.org/record/4059940/files/A_79_263-EN.pdf.

stigmatizing language, targeting both the funding organizations and the civil society organizations themselves, as well as their staff, reinforcing stigmatization and exposing them to hate speech, defamation, and attacks.

6. Dual-use Technology in the Context of the Military-Industrial Digital Complex: The Increasingly Blurred Civilian-Military Demarcation

The rapid development of advanced conventional weaponry and military technology since the 1990s has occurred during a period when militarily relevant technologies have become increasingly difficult to identify and classify. Many advanced commercial technologies offer new and potentially significant opportunities for defense applications, thus impacting military power and metrics of military superiority. Even before the end of the Cold War, technologies and technological innovations designed and developed in the commercial high-tech sector were clearly superior and less expensive than those found in the military-industrial complex.[174] This superiority of commercial technologies has become even more apparent in recent years with the emergence of the fourth industrial revolution, which revolves around new technologies such as artificial intelligence, autonomous systems, big data, and quantum computing. At the same time, these technologies and their associated products are making the distinction between military and civilian technology—and, more broadly, the distinction between military- and civilian-based innovation—ever more difficult to distinguish.[175] With these developments, the boundaries between the civilian and military sectors are increasingly blurring, particularly in the areas of space, cyberspace, and artificial intelligence. The increasingly blurred demarcation between civilian and military landscapes is driving a new era of civil-military collaboration that is poised to change the face of national security and technological innovation.[176]

Along with these developments, concerns about dual-use technologies emerged alongside fears of the proliferation of nuclear weapons-related technologies at the beginning of the Cold War. These concerns focused on well-defined targets, such as specialized steels, high-precision computer-aided manufacturing tools and facilities, and high-performance software and hardware; including materials and devices readily adaptable for nuclear weapons-related design and manufacturing. More recently, the focus has shifted to the context of non- nuclear technologies, including biological and information technologies, whose ongoing research and development dramatically improves human social and economic well-being, albeit at the expense of the potential for these technologies to be exploited for nefarious purposes.[177]

The term “dual-use” originally referred to a specific set of nuclear materials after World War II that could be used for both military (weapons) and civilian (energy) purposes. Today, the term is applied more broadly to include companies whose products can meet government needs. The Export Administration Regulations define dual-use goods as goods that have both civilian applications and potential uses in terrorism, the military, or weapons of mass destruction. In investment contexts, such as the European Investment Fund, dual-use investments are now accepted as long as they exclude arms and ammunition. However, distinguishing between technologies for civilian and military use has become increasingly challenging as the line

[174] Yoram Evron and Richard A. Bitzinger, *The Fourth Industrial Revolution and Military-Civil Fusion: A New Paradigm for Military Innovation?* (Cambridge: Cambridge University Press, 2023).

[175] In particular, the later stages of the so-called third industrial revolution – centered on breakthroughs in microelectronics, computing, telecommunications, and other information technologies – were largely dominated by innovation centered in the commercial sphere, for example, in places like Silicon Valley or Israeli technology incubators, or in companies like Google, Amazon, and Alibaba. See, Evron and Bitzinger, *The Fourth Industrial Revolution and Military-Civil Fusion*.

[176] Gonçalo Lopes, “From Orbit to Cyber Wars: The New Era of Civil-Military Synergy,” *VisionSpace*, March 25, 2025, https://visionspace.com/from-orbit-to-cyber-wars-the-new-era-of-civil-military-synergy/.

[177] Robert Rosner, “Preface,” in *Governance of Dual-Use Technologies: Theory and Practice*, edited by Elisa D. Harris (Cambridge, MA: American Academy of Arts and Sciences, 2016).

between offensive and defensive solutions has become increasingly blurred. Further implications: for some investors, deciding where to draw the line between supporting technologies for war or peace remains a complex and contentious issue.[178]

Jake Chapman defines dual-use technology by considering four more specific categories, including: [179]

1) Commercial/Commercial:

The use of this technology, including technology developed for the commercial market, remains largely commercial in nature. This use of technology is called commercial off-the-shelf technology.

These can take the form of hardware or software already commercially available for sale to the public. These technologies are readily available because they are designed to meet stringent industry standards and involve substantial private investment. The use of these technologies leads to solutions that are continually being refined and can be adopted at low cost and scaled up.

2) Defense/Commercial

These technologies originated in the defense field but have substantial future commercial markets. This category encompasses many dual-use technologies that are the foundation of Silicon Valley, but are becoming less and less visible in the tech ecosystem each year. Technologies currently under development could be considered Defense/Commercial, including hypersonic flight and advanced methods for positioning, navigation, and timing, such as advanced devices for the Global Positioning System (GPS). This category is not the technology most sought after by venture capital investors, nor is it what most people in defense innovation are talking about under the dual-use umbrella;

3) Defense/Defense

Prime contractors, in turn, have traditionally focused on defense-derived technologies and will largely remain focused on the defense market. This category includes innovative munitions, all advanced platforms such as fighter aircraft, bombers, and ships, as well as highly specialized applications of specific technologies, such as artificial intelligence. This category is only dual-use technology in the most liberal definition and tends to receive the least private venture capital funding.

4) Commercial/Defense

While all of the above categories describe capabilities that are technically dual-use, this technology category prioritizes commercial first and defense second. This category has received attention from both the venture capital and defense communities, particularly in the United States. This technology category is vulnerable to hacking. The United States Department of Defense is increasingly promoting dual-use commercial/defense technologies through startups. Startups are encouraged to develop commercial products first and successfully develop businesses in the commercial market. Once startups achieve sufficient commercial success to survive the maze of defense acquisitions, they can then pursue to adapt their product for the military.

Meanwhile, according to Gene Keselman and Fiona Murray, dual-use technology is a market strategy that may be implemented with a focus on defense, commercial use, or both. Currently,

[178] Defining “Dual Use”|Dual-Use Readiness Model (https://dualuse.mit.edu/defining-dual-use/), accessed on August 19, 2026

[179] Jake Chapman, Reliance on Dual-Use Technology Is a Trap (https://warontherocks.com/reliance-on-dual-use-technology-is-a-trap/), accessed on August 28. 2026

the term is used loosely to encompass a wide range of companies whose products and services can solve both military and civilian problems. In the investment context, major funders such as the European Investment Fund have excluded ventures developing dual-use solutions for defense. Others only consider these ventures worthy of support if commercial markets are explored first or constitute the majority of sales. Over time, each of these boundary conditions has become increasingly eroded. According to the European Investment Fund, the boundaries of so-called dual-use investments are now drawn only to exclude ammunition and weapons. At the same time, the dual-use technology category continues to confuse investors and the market due to the lack of a clear and useful definition for establishing a clear and measurable corridor.[180]

On the other hand, for investors, dual-use technology should be understood as a strategy that will shape plans and priorities and emphasize ethical adoption in all use cases of the technology. A dual-use strategy, regardless of whether it prioritizes defense or runs parallel with civilian use cases, like other market entry strategies is related to trade-offs: which solution to build and for whom, how to test it, how to fund it, and how to implement it appropriately. Furthermore, Gene Keselman and Fiona Murray, identified three dimensions for examining dual-use technology, including: (1) customer dimension; (2) funding dimension; and (3) technology dimension.[181] A description of the three dimensions of dual-use technology can be seen in the table below.[182]

Table 2

Dimensions of Dual-Use Technology	Description
Customer	The commercial and defense markets are very different. Commercial markets typically feature intense competition, a focus on rapid innovation, and a direct relationship between customers and products. Manufacturers have demanding customers and a focus on economic efficiency. In contrast, military markets often operate in a more structured environment, with long timeframes, stringent regulations, and complex stakeholder networks. Government customers operate under a complex set of regulations and with specialized vocabulary.
Funding	Commercial ventures often rely on dilutive capital, that is, funding from individual investors or venture capitalists (institutional investors) by taking equity shares in the venture. Government funding, also known as non-dilutive funding, can take the form of grants and contracts from specific government agencies. While this funding typically does not require the relinquishment of equity or ownership, it often involves contractual complexity. Government funding can provide the opportunity to support some research and development, with later stages typically involving larger funding. However, this involves a maze of regulations and compliance requirements, including the scope of work and expected outcomes.

[180] Gene Keselman and Fiona Murray, "Dual-Use Is a Strategy, Not a Category (Nor a Trap)," *War on the Rocks*, January 2, 2025, https://warontherocks.com/dual-use-is-a-strategy-not-a-category-nor-a-trap/.
[181] Keselman and Murray, "Dual-Use Is a Strategy, Not a Category."
[182] Keselman and Murray, "Dual-Use Is a Strategy, Not a Category."

Technology	While the basic solutions may be similar for commercial and defense contexts, the way technological progress is described and measured can differ significantly . In the broader defense and government context, technology must meet stringent specifications, requirements, and standards, such as military specifications and technology readiness levels. While the goal is to acquire capabilities that meet mission needs, these precise technology requirements are designed to ensure compatibility and effectiveness within the broader mission system. Mission users expect evidence of progress through formal processes such as field trials, operational testing and evaluation, and simulations such as war games that replicate real-world scenarios.

The logic of dual-use technology is not new; militaries have always targeted civilians and civilian space to gain an advantage over their belligerents.[183] With the important historical precedent of war, it was from this context that a series of humanitarian legal infrastructures based on the distinction between civilians and combatants were formulated and revised, as well as international governance mechanisms such as international criminal law, the International Court of Justice, the International Criminal Court, and international humanitarian law. The 1949 Geneva Conventions and their 1977 Additional Protocols governing humanitarian law were designed precisely to prevent the collapse of the civilian and military categories. This lack of distinction between civilian and military categories underpinned the devastation of the Second World War and the violence of subsequent wars in the 1950s and 1960s. The principle of distinction[184] asserts that participants in a conflict 'must at all times distinguish between civilians and combatants and between civilian objects and military objectives and shall therefore direct their operations only against military objectives.'[185] These technologies are increasingly central to national security, economic resilience, and technological leadership. Dual-use technology is becoming increasingly important for a country's economic growth and its ability to defend itself. This technology is crucial for boosting competitiveness, resilience, and crucial national defense and security, especially in today's threatening international geopolitical environment.[186]

Among the areas in which the distinction between military and security equipment production has been eroded[187] is the increasing importance of civilian technology and dual-use items in these areas. States and arms manufacturers are expanding the range of situations in which civilian technology can be used in the production of military and

[183] In military history, dual use has been a mainstay of warfare; for example, Allied and German air forces both bombarded European cities during World War II, and the United States Air Force targeted villages, towns, and cities during its campaigns in Vietnam, Laos, and Cambodia. These wars were characterized by forms of military violence that either did not distinguish between civilian and military space or, conversely, exploited that distinction as a means to demoralize the enemy. See, Jones, Mousamputri, and Griffiths, "Dual Use as a Political Technology of Contemporary Military Violence."

[184] The principle of distinction is the most important legal principle of war, underlying all other principles. For example, the principle of proportionality, which balances military objectives and needs with potential harm to civilians and civilian objects, relies entirely on identifying and then defining the nature of civilians. See Jones, Mousamputri, and Griffiths, "Dual Use as a Political Technology of Contemporary Military Violence."

[185] Jones, Mousamputri, and Griffiths, "Dual Use as a Political Technology of Contemporary Military Violence."

[186] Hinton, *Dual-Use Technologies in the Age of Intangibles*.

[187] Military and security equipment, that is, equipment developed and used for military and security purposes by armed forces, law enforcement agencies, intelligence agencies, and private security companies. See Hinton, *Dual-Use Technologies in the Age of Intangibles*.

security equipment. As a result, technologies and systems previously classified as civilian may need to be reclassified as dual-use items, that is, goods, software, and technologies that can be used for both civilian and military applications. Countries are also encouraging companies, research and academic institutions to develop technologies and systems that are 'dual-use' by design and can be incorporated into military and security devices or used as military and security equipment. This process can create a new category of dual-use goods.[188]

This shift creates new risks for governments, companies, and the research and academic institutions involved. The expanding scope of situations where civilian technology is incorporated into military and security equipment, and the creation of technologies and systems that are dual-use by design, are creating new pathways for the production of military and security equipment. This also increases the reach of companies, research and academic institutions directly or indirectly involved in the production of military and security equipment. This shift creates new pathways for military and security equipment to reach criminals, terrorists, or states that might use it in connection with violations of international human rights law or international humanitarian law.[189] This shift and the risks it poses are exemplified in the case of facial recognition technologies, a type of biometric technology that can be used to identify a person based on facial features. These technologies have been primarily developed in the civilian sector and have a wide range of civilian applications, but are also being integrated into military and security equipment. Concerns about the risks of diversion and misuse have been raised regarding facial recognition technologies and military and security equipment that incorporate them.[190]

Similarly, space is no longer the exclusive playground of governments. Contemporary military operations increasingly rely on private satellite companies that provide intelligence and communications services worldwide. Satellites can now be used to support battlefield coordination and military operations. A satellite providing internet access to civilians can, at the same time, enable military control.[191] Since the Cold War, military satellites have been used to establish secure communication channels, for maneuvering and coordinating military forces, and for targeting missiles. However, there are different uses for satellites, not directly related to military operations, namely for intelligence, surveillance, and reconnaissance purposes. In intelligence, surveillance, and reconnaissance activities, civilian satellites are valuable sources of data and information. Meteorological satellites provide weather information crucial for the conduct of operations without the risk of loss caused by atmospheric conditions. Scientific and commercial satellites can sell their services to armed forces, thus providing data without being under direct military control. In all these applications, satellites indirectly become instruments of war. However, satellites are not used as weapons platforms, as this would violate the current international consensus against the militarization of space. Although the provisions of the 1967 Outer Space Treaty explicitly prohibit the deployment of weapons of mass destruction and the construction of military installations, the treaty does not regulate the use of satellites as

[188] Mark Bromley and Giovanna Maletta, The Militarization of Technology: Preventing Diversion and Misuse Through Export Controls, *SIPRI Research Policy Paper* (Stockholm: Stockholm International Peace Research Institute (SIPRI), November 2025), https://doi.org/10.55163/VDOD7802.

[189] Bromley and Maletta, The Militarization of Technology.

[190] Certain types of facial recognition technology and military and security equipment incorporating facial recognition technology are already covered by state export controls. The European Union (EU) and the United States have also discussed creating a new category of export controls to capture this technology. See Bromley and Maletta, *The Militarization of Technology*.

[191] Sofia Niiles, "Dual-Use Satellites and the Law of Armed Conflict: The Tension Between Targeting Rules and State Responsibility in Outer Space," *Amsterdam Law Forum*, June 10, 2026, https://vu.nl/en/news/2026/dual-use-satellites-and-the-law-of-armed-conflict.

indirect instruments of war. Therefore, any attempt to regulate their use in warfare must take into account the inherent dual nature of satellite data.[192]

Elon Musk's intervention during Russia's invasion of Ukraine is one example of how space technology has changed the course of armed conflict. Musk, through his company, Starlink, provides communications infrastructure and surveillance capabilities to Ukrainian and Russian forces. However, Musk has consistently restricted access to these services on both sides, highlighting how a single private actor can influence military operations that were previously managed by states.[193] Starlink's dual role as both technological infrastructure and geopolitical tool is a stark reality in Gaza. Since October 2023, Israel's relentless bombardment has destroyed most of the territory's communications network, leaving hospitals, ambulances, and aid agencies without power. Starlink's involvement in Gaza, when Israel targeted Gaza's telecommunications infrastructure, causing a power outage for 2.3 million Palestinians, was quickly activated for the Israeli Defense Forces (IDF). The Israeli army has killed an estimated 60,000 Palestinians, mostly women and children. Then, on October 27, a total Israeli communications blackout in Gaza prompted Elon Musk to pledge Starlink support to internationally recognized aid organizations.[194]

This situation demonstrates the blurring of the military and non-military realms of political technology to legitimize military violence. At times and to varying degrees, in war zones, everything can be targeted or prohibited, everyone is guilty and can be killed; hospitals are military warehouses, building materials are bomb components, and civilians are combatants. Almost everything is subsumed within the logic of warfare and thus almost everything can be destroyed, from people and homes to life-sustaining medicines and food. Dual-use technology has become a crucial political technology central to the distribution of contemporary military violence.[195]

Today, states and militaries have used the dual-use framework of International Humanitarian Law to enable operations in both the civilian and military spheres, thereby amplifying the impact of war. In the use of law for war purposes (lawfare), legal principles and arguments are repurposed or manipulated in ways that justify enabling rather than limiting military violence. At the forefront of lawfare innovation, for example, among military lawyers in the United States and Israel, law has become a force multiplier, operating in gray areas to enable increasingly destructive military violence that relies on shifting definitions of dual-use. Examples of lawfare and the instrumentalization of dual-use are numerous.[196]

In this context, the militarization of technology, according to Mark Bromley and Giovanna Maletta, is a broad term used to refer to a set of interrelated processes that are eroding the conventional distinction between how civilian technology and military and security equipment are produced and used. These processes include the deployment of data-intensive systems for military purposes, a situation that places companies and startups that have developed commercial and civilian infrastructure technologies into the defense sector, and the reuse and adaptation of technologies developed for use in conflict zones for commercial purposes.[197] Privacy International identifies a trend of battlefields shifting towards cities as the technologies

---

[192] Danilo delle Fave, "The Challenges of Dual-Use Space Technologies: The Non-Peaceful Use of Satellites," *Space Generation Advisory Council*, April 14, 2023, https://spacegeneration.org/the-challenges-of-dual-use-space-technologies-the-non-peaceful-use-of-satellites.

[193] Alyssa Macaluso, "Space Is Not a Human Rights Vacuum," *Science & Politics*, February 25, 2026, https://sciencepolitics.org/2026/02/25/space-is-not-a-human-rights-vacuum/.

[194] Rushad Faridi, "Starlink in Gaza: Humanitarian Lifeline or Military Asset?" The Daily Star, September 9, 2025, https://www.thedailystar.net/slow-reads/focus/news/starlink-gaza-humanitarian-lifeline-or-military-asset-3981756.

[195] Jones, Mousamputri, and Griffiths, "Dual Use as a Political Technology of Contemporary Military Violence."

[196] *Ibid*.

[197] Mark Bromley and Giovanna Maletta, *op.cit*.

we rely on every day are militarized. In turn, civilian technologies driven by data and human life are moving to the battlefield. The same companies that build war devices are expanding to provide civilian infrastructure, and vice versa.[198] According to Privacy International this phenomenon is seen in various forms:[199]

1. Countries are bringing military technology into urban centers by partnering with the defense technology industry, called the militarization of civilian spaces;
2. Civilian tech companies are entering the battlefield, bringing civilian data with them, which is called the militarization of civilian tech;
3. Companies and private investment funds are pouring in unimaginable amounts of money, creating incentives for surveillance and war, and prioritizing investors over the people, known as the privatization of military tech.

This situation illustrates a military-industrial complex that brings together a vast web of interests held by the military, defense contractors, and others with a stake in the business of war and armed violence. As financial and political interests in war spread among military leaders, defense contractors, politicians, lobbyists, universities, and think tanks, the modern concept of the military-industrial complex has become increasingly broad and ill-defined. On the other hand, the modern defense industry itself has become difficult to define, encompassing everything from mercenaries to weapons manufacturing to information technology services. With companies like Boeing, Palantir, Oracle, and others serving both military and civilian markets with dual-use technologies, the defense industry appears increasingly difficult to differentiate.[200]

Further impacts include the increasingly blurred boundaries between military and civilian sectors, which pose a serious risk that technological development in one context will be transferred to another without considering the different rules of engagement. There is a significant risk if both sectors are allowed to continue exploiting loopholes in legal instruments and oversight. This will result in greater exploitation, a greater concentration of power, and encourage continued militarization.[201]

In this context, the term military-industrial is too narrow to describe this phenomenon. This term does not fully address the strengthening of the politics and culture of war, normalized through everything from defense-sponsored university research to military recruitment embedded in popular culture.[202] The military sector is a realm where the boundaries between states and corporations can become extremely blurred. With the digitalization of the global economy, this overlap is becoming increasingly intense. Controlling digital networks and chokepoints flowing from one continent to another allows for weaponizing interdependencies, providing a significant advantage over both enemies and allies. However, this is nearly impossible without the support of Big Tech companies. Without Big Tech, the global network could hardly be weaponized.

Big Tech's role is becoming increasingly dominant as contemporary warfare becomes increasingly digital. For example, an artificial intelligence-powered drone selling for less than US$100,000 can easily destroy an aircraft or tank costing 100 times as much. Advanced cloud and satellite communications systems are crucial for gathering information and preventing or

[198] Privacy International, *loc.cit.*
[199] *Ibid*.
[200] Kaitlyn Church, "The Military-Industrial Complex: Why This Is of Importance to Action on Armed Violence and What It Has to Do with the Erosion of Civilian Protection," *Action on Armed Violence (AOAV)*, July 14, 2026, https://aoav.org.uk/2026/the-military-industrial-complex-why-this-is-of-importance-to-action-on-armed-violence-and-what-it-has-to-do-with-the-erosion-of-civilian-protection/.
[201] Privacy International, "Challenging the Militarization of Tech."
[202] Church, "The Military-Industrial Complex."

executing physical and cyberattacks. Even the performance of conventional weapons, such as aircraft, tanks, and anti-aircraft systems, is highly dependent on their digital components.[203]

Over the past decade, the well-known concept of the military-industrial complex, coined by Eisenhower in 1961, has evolved into a new hybrid form: the digital-military-industrial complex. This variant centers on companies specializing in data, artificial intelligence, and digital platforms, as well as startups that have deliberately positioned themselves as providers of defense-oriented technologies. These entities are collaborating closely with the U.S. military and conventional defense contractors to accelerate the digitization and intelligence-driven transformation of military capabilities. This digital variant could lead to large-scale interventions by the United States abroad, potentially transforming it into a new war machine.[204]

Conventional defense giants like Lockheed Martin, Raytheon, Northrop Grumman, and General Dynamics now face fierce competition from two types of digital industry players. The first category includes tech giants like Microsoft, Amazon, Google, Oracle, HP, Dell, Motorola, IBM, and others, many of which have won substantial Pentagon contracts to supply advanced systems software, cloud, data, and artificial intelligence services. The second category consists of venture capital-backed startups, often funded by Silicon Valley investors, focusing on artificial intelligence, autonomous systems, sensing technologies, and network-based command and control systems specifically designed for military and intelligence needs. These startups prioritize national security as a key attribute of their products in an effort to capture market share in the United States' defense procurement market.[205]

From a corporate perspective, there are advantages to expanding these activities. First, at a time of heightened concerns about global conflict, particularly in Ukraine and the Middle East and great-power rivalry, some technology executives and their companies are being seen as guardians of US national security. Second, as major tech companies expand their contracts with the Pentagon, they are able to tap into a highly lucrative and relentlessly growing revenue stream.[206] In late 2022, the Pentagon announced a $9 billion contract for the Joint Warfighting Cloud Capability (JWCC) initiative, jointly awarded to Microsoft, Google, Oracle, and Amazon. The deal clearly demonstrates the tech industry's commitment to working with the Pentagon. It addresses concerns about the so-called cultural divide between Silicon Valley and Washington. The program's goal is to provide cloud computing services at mission-level speed, across all classification levels, from headquarters to the tactical edge. Despite ongoing employee protests against military contracts, such as Project Nimbus, Google and Amazon's cloud computing contract with the Israeli government that includes facial recognition, video analytics, and sentiment analysis capabilities, company executives have continued with them.[207] According to the Report of the Special Rapporteur Francesca Albanese on the situation of human rights in the Palestinian territories occupied since 1967, Microsoft, Amazon, and Google are among the major companies identified as part of a joint criminal enterprise in aiding Israel in carrying out genocide in Gaza.[208] These companies have

[203] Coveri, Cozza, and Guarascio, "Big Tech and the US Digital-Military-Industrial Complex."
[204] Shi Bowei, "The Rise of the US 'Digital-Military-Industrial Complex,'" *China Daily*, October 20, 2025, https://www.chinadaily.com.cn/a/202510/20/WS68f599c6a310f735438b5e2d.html.
[205] Bowei, "The Rise of the US 'Digital-Military-Industrial Complex.'"
[206] González, *How Big Tech and Silicon Valley Are Transforming the Military-Industrial Complex*.
[207] González, *How Big Tech and Silicon Valley Are Transforming the Military-Industrial Complex*.
[208] Francesca Albanese, *From Economy of Occupation to Economy of Genocide*, *Report of the Special Rapporteur on the Situation of Human Rights in the Palestinian Territories Occupied since 1967*, UN Doc. A/HRC/59/23 (United Nations, 30 June 2025), https://www.ohchr.org/en/documents/country-reports/ahrc5923-report-special-rapporteur-situation-human-rights-palestinian.

earned untold profits from the unprecedented massacre of more than 62,000 Palestinians since October 2023.[209]

Tech for Genocide continues to advance. Newer artificial intelligence tools, modeled on generative platforms, such as ChatGPT, are being developed by Israeli intelligence to expedite surveillance, prosecution, and arrest. These experiments are not isolated and limited to the Gaza genocide. They project the future of automated warfare, developed in collaboration with and supported by major US tech companies. Israel's role as a laboratory for US imperialism connects all of this. Every tool of occupation tested on Palestinians becomes a global export. Predictive policing software pioneered in the West Bank is sold to US police departments. Biometric checkpoints tested in East Jerusalem appear on the US-Mexico border. Artificial intelligence surveillance tested in Gaza is marketed to authoritarian regimes around the world. For Big Tech, Israel is both a lucrative client and a testing ground. By embedding themselves within the Israeli military machine, Microsoft, Google, Amazon, and Palantir are jointly developing repression technology that can be scaled and sold worldwide. The destruction of Gaza has become not just a geopolitical project, but a business model. The marriage of Big Tech and the military-industrial-surveillance complex has been perfected. Israel is at the forefront of this project, but its scope is global. From Gaza to Ukraine, from Baghdad to San Diego, the same companies are profiting from surveillance, targeting, and repression.[210]

In this context, Craig Jones, Ichamati Mousamputri, and Mark Griffiths define dual-use discourses and infrastructures as discursive, material, and relational networks that position people, places, and things identifiable as military and civilian, as well as the processes of making and unmaking distinctions between military and civilian. In this context, the military world and civilian life is separated from two opposing perspectives. First, from a humanitarian and legal perspective, to codify civilian space in a way that counters dual-use technology.

Second, in the dual-use instrumentalization to legitimize military violence against civilian sites and bodies. On the one hand, especially from the perspective of human rights and international law, there are efforts to demarcate non-military space from military targets with the aim of protecting civilian lives. On the other hand, there are military approaches to blur these boundaries, often by focusing on combatants' claims of using civilians as human shields and that civilian objects and places can be used for military purposes.[211]

This shift in the center of the military industrial complex has prompted stakeholders to pay attention to several things:[212]

1. There is a blurred line between civilian and military technology.

---

[209] Israel's apartheid and military systems require ever-increasing cloud computing and storage capacity. The Israeli government and military cloud computing project known as Project Nimbus, which secured a $1.2 billion contract with Google and Amazon in 2021, is designed to meet this need. Even when the Israeli military's internal cloud computing was overloaded in October 2023, Microsoft, Google, and Amazon stepped in to provide critical cloud and AI technology. IDF computer chief Colonel Racheli Dembinsky described the platform as a weapon, describing cloud technology as part of the IDF's suite of systems. See Progressive International, "UN Calls Out Google and Amazon for Abetting Gaza Genocide," August 26, 2025, https://progressive.international/wire/2025-08-26-un-calls-out-google-and-amazon-for-abetting-gaza-genocide/en/.

[210] Bappa Sinha, "Big Tech's Deep Links With Genocide in Gaza," *NewsClick*, October 6, 2025, https://www.newsclick.in/big-techs-deep-links-genocide-gaza.

[211] Jones, Mousamputri, and Griffiths, "Dual Use as a Political Technology of Contemporary Military Violence."

[212] UN B-Tech Project, Heartland Initiative, Business & Human Rights Resource Center, and Open MIC, *Key Takeaways: Dual-Use Dominance When Every Innovation Has a Defense Application*, 26 July 2025, https://www.ohchr.org/sites/default/files/documents/form/defense-application-key-takeaways-25-internet-governance-forum-side-event-dual-use-dominance-innovation-1-en.pdf.

The boundary between technology companies and the defense sector is increasingly blurred. Technology companies that once distanced themselves from military involvement are now key actors. This includes companies abandoning previous commitments to avoid producing artificial intelligence products for military purposes. The concept of dual use remains poorly defined and its application is inconsistent. This ambiguity makes it difficult for investors and the public to evaluate the risks associated with technology products used in military contexts.[213]

2. Limited accountability and responsibility remain a major problem
   Stakeholders highlighted the lack of meaningful accountability for technology companies, which poses serious risks. Accountability is a structural issue that extends beyond a single company as risks extend to third-party vendors and infrastructure providers. Dominant geopolitical narratives, particularly those focused on international technological competition, contribute to increased risk tolerance within defense agencies. The military may overlook vulnerabilities or move forward with systems that fail legal review. There is little transparency regarding when companies collecting civilian data can reuse it to train military-focused AI systems, which has serious implications for consent and privacy.[214]
3. Conventional (traditional) due diligence tools are inadequate for this context.
   Conventional investor approaches may not fully capture the risks posed by multi-purpose technologies. As technology companies expand into the defense sector, they often lack a sufficient understanding of military responsibilities. New devices such as artificial intelligence and cloud computing infrastructure often fall outside conventional weapons classifications. Basing assessments on international humanitarian law offers a clearer legal and ethical foundation but requires active investor engagement beyond environmental, social, and governance standards.
4. Compliance with export controls alone is not enough
   Compliance with export control regimes cannot be considered adequate due diligence, particularly in the context of multi-purpose technologies. While arms export laws cover some defense-related cases, they have been described as unreliable in consistently identifying high-risk technologies. Export permits often reflect political alliances rather than human rights considerations.
5. Going forward, a number of steps need to be taken.
   Addressing the human rights risks associated with multi-purpose technologies requires more than just general principles. Some argue that the UN Guiding Principles (UNGPs) are sufficient, while others advocate additional guidance that addresses how the framework applies to dual-use contexts.

The focus of this attention can be placed on three issues of dual-use technology governance. First, there is a difference in awareness of the governance challenges of the three different

[213] Within the framework of international humanitarian law, the distinction is clearer, with assets classified as civilian or military based on their use, not their design or intent. The notion of legal gray areas should be discarded; instead, legal clarity should be widely adopted by companies and investors when assessing their roles and responsibilities, rather than relying on an assumption of neutrality. Some technology companies deliberately pursue contracts with governments widely criticized for human rights violations. Many companies agree to conduct human rights impact assessments but avoid doing so in the military context. This reflects a lack of transparency. With the availability of artificial intelligence tools, open-source intelligence, and civil society reporting, companies can conduct stronger due diligence across their value chains and are required to conduct more rigorous human rights due diligence when their technology is used in conflict-affected areas. See, UN B-Tech Project et al., *Key Takeaways: Dual-Use Dominance When Every Innovation Has a Defense Application*.

[214] Dual-use weapons systems or technologies increasingly minimize the role of humans by simply executing predetermined outcomes generated by artificial intelligence. This reduced role further complicates accountability structures. See, UN B-Tech Project et al., *Key Takeaways: Dual-Use Dominance When Every Innovation Has a Defense Application*.

domains of dual-use technology. For example, while there is general international agreement on the need to restrict access to nuclear weapons development technology, there is no such consensus in the biological and information technology domains. In fact, in biotechnology research, there is considerable opposition from the biological sciences community to any attempt to restrict access to or dissemination of research findings, including information that could cause significant harm. Meanwhile, in the information technology arena, this is largely ignored. In some cases, information technologies routinely infiltrate each other's networks to obtain network intelligence and information, including the identification of vulnerabilities that could allow for future exploitation.

Second, an effective governance model assumes the ability to identify and punish violators of its provisions. While some degree of attribution is possible in the nuclear field, attribution in the biological field is far more complex and may be practically impossible in the case of information technology. And third, the problem of law enforcement confounds even the most easily understood dual-use device field.[215]

Changes in dual-use technology governance need to be placed within the context of military-civilian fusion within the fourth industrial revolution. According to Yoram Evron and Richard A. Bitzinger, this military-civilian fusion is based on the following argument:

1. The technologies associated with the emerging Fourth Industrial Revolution are increasingly understood to be fundamental determinants of future military effectiveness and superiority. Like the Third Industrial Revolution, the Fourth Industrial Revolution is largely based on digital technologies, and in particular information technologies, such as microelectronics, computing, software, and the like. However, the Fourth Industrial Revolution goes beyond the Third Industrial Revolution. It focuses on the collection, storage, and processing of data, but on a much larger scale than was envisioned at the time of its development. Like the Third Industrial Revolution, the Fourth Industrial Revolution is about communications and networking, but on a much greater scale, complexity, and intensity in terms of connectivity, sharing, and togetherness. Above all, the Fourth Industrial Revolution is about processing power, storage capacity, and unlimited access to unprecedented knowledge, connecting people and things while producing a fusion of technologies that blurs the boundaries between the physical, digital, and biological realms;
2. Efforts to harness the potential of fourth industrial revolution technologies require the military to create new forms of civil-military cooperation in science and technology. Since the late 2010s, this strategy has become known as military-civil fusion, a form of military-civil cooperation that has been increasingly recognized as a key mechanism for the military's assimilation of fourth industrial revolution technologies. Military-civil fusion gained strength after the Cold War when the civilian sector overtook the military as the most important source of innovative technologies. Military-civil fusion is concerned with providing the military with technological innovations that originally originated in the commercial sector. Contemporary military-civil fusion focuses on cutting-edge commercial technologies, particularly fourth industrial revolution technologies, that can then be adapted and integrated into military systems and can provide significant advances in military capabilities. At the same time, military-civil fusion goes beyond simply discovering and assimilating civilian technologies. It also involves designing strategies and initiatives to discover adequate civilian technologies and their production, then leveraging them for military research and development projects, engaging the military in research and development collaborations with civilian entities.

[215] Rosner, "Preface."

This can be interpreted as meaning that cyberspace has reshaped the conceptual and institutional foundations of civil-military relations. According to Isabella Neumann, cyberspace has destabilized authority, broken down coordination, increased politicization, and expanded the influence of the private sector, deepening the state's dependence on civilian capabilities. Within military organizations, hierarchies are reconfigured around technical expertise, suppressing authority and intensifying competition. Beyond the military, the vulnerability of shared infrastructure binds the civilian and military spheres, while digital platforms reshape legitimacy and public trust. The framing of cyberspace as a domain of warfare further extends military influence into civil governance.[216] Furthermore, Isabella Neumann identifies three conclusions for examining military-civilian relations in the context of cyberspace:[217]

1. Cyberspace operates as a transversal condition that permeates multiple dimensions of civil-military relations, changing both the distribution of capabilities and the location and character of authority itself. Therefore, the uniqueness of cyberspace lies in how it reconfigures interactions across core dimensions of civil-military relations. Even developments in one domain reverberate across other domains in cyberspace, producing recursive feedback loops that blur distinctions and deconstruct linear or compartmentalized understandings of civil-military relations;[218]
2. Considerations regarding the militarization of the cyber realm will be accompanied by civilian control and the shift of expertise to civilians and the private sector. This poses challenges to civilian supremacy and democracy because control over crucial capabilities is fragmented and cannot be easily consolidated within military institutions. Conventional militarization involves the gradual extension of military logic, personnel, or tools into the civilian realm. However, in the cyber realm, militarization takes a different form. Military actors extend their reach into the information environment and digital infrastructure. Consequently, classic patterns such as centralized command, hierarchical discipline, and control over the instruments of state power cannot be easily replicated in the cyber realm. Civilian control may be affected by cyber technology, as military cyber capabilities are deeply entrenched and persist beyond regime change.
3. Cyberspace reveals fundamental tensions between established civil-military institutional logics and the operational requirements of the domain. Effective governance requires distributed expertise, rapid information exchange, and sustained cross-sector collaboration, making the standard organizational forms of vertical command structures, rigid civil-military demarcations, siloed intelligence systems, multi-year acquisition timelines, and hierarchical strategic planning processes less suited to the cyber realm. These dynamics suggest broader implications. Existing civil-military relations frameworks struggle to account for forms of interaction defined by interdependence, simultaneity, and diffusion. This, therefore, calls for a rethinking of the conceptual foundations for understanding civil-military relations.

---

[216] Neumann, "It Is Complicated: Cyber into the Civil–Military Relationship."

[217] Neumann, "It Is Complicated: Cyber into the Civil–Military Relationship."

[218] The operational demands of cyberspace, including technical expertise, flexibility, and continuous coordination, draw civilian and military actors into closer interactions, blurring the lines between political and military roles. Externally, this opens up space for non-state actors, including private companies, technical communities, and hybrid entities, to serve as nodes of authority in governance networks. Military-civilian relations, at the same time, are reshaped through shared vulnerabilities and symbolic contestations. In general, authority becomes partially understandable but overall opaque, hampering conventional mechanisms of oversight and accountability. Within military organizations, cyber triggers a series of institutional effects as it flattens hierarchies by shifting analytical and decision-making capacities away from senior ranks. The distinctiveness of cyberspace, therefore, lies in how it reconfigures interactions across core dimensions of civil-military relations. See, Neumann, "It Is Complicated: Cyber into the Civil–Military Relationship."

Based on these three conclusions, Isabella Neumann identifies thematic categories from a cybersecurity perspective that cut across the pillars of civil-military relations:[219]

Table 3

Thematic Categories	Representative Cases
Traditional Pillars	
§ Military coup	-
§ Democratic transition	-
§ Civilian control	Grey zone operations that blur the lines between peace and conflict; destabilization of traditional authority structures; failure of coordination between civilian institutions and military cyber commands; increased risk of politicization; and the influence of private sector actors on national cyber defense.
Contemporary Pillars	
§ Non-state actors	Hybrid crises and multi-domain threats; state reliance on civilian and private sector cyber capabilities; proliferation of offensive cyber tools by proxy groups; private technology companies operating as critical nodes in national cyber defense.
§ Military Organization Studies	Restructuring of command hierarchies based on technical expertise; compression of authority as the operational significance of junior personnel increases; interorganizational competition over ownership of the cyber mission; cultural adaptation; cognitive biases in cyber countermeasures decision-making; recruitment and retention challenges in a competitive technical labor market.
§ Military-society relations	The shared vulnerability of civilian and military infrastructure to cyberattacks; the military's use of digital platforms for legitimacy and narrative management; the erosion of public trust following high-profile data breaches; the blurring of the distinction between civilian and military targets in cyber conflict.
§ Politicization	The military's framing of cyberspace as a domain of warfare; doctrinal concepts that extend the military's relevance to the civilian realm of governance; cyber platforms that intersect with electoral politics and political debate; legal and conceptual ambiguities that create room for military interpretation.

[219] Militarization in the cyber domain, when placed with elements of civilian control and the relocation of expertise to civilian actors and the private sector, can help explain why some conventional pillars of the field, such as military development and democratic transition, require separate analysis. It suggests that while the military's presence may expand in the cyber domain, the spread of expertise and capabilities among non-military actors makes military defiance impossible, as control over capabilities is fragmented and cannot easily be consolidated within military institutions alone. This creates a paradoxical dynamic: the military's operational footprint extends into the cyber domain but its relative authority over the cyber domain precludes full control. See ibid.

§ Militarization	Establishment of a dedicated cyber command; normalization of sustained engagement and advanced defense doctrine; bureaucratic competition for cyber resources and institutional prestige; the extension of military logic into the protection of civilian infrastructure.

When examining the pillars and cases that represent each contemporary pillar of military-civilian relations in the cyber context, governance issues become crucial for mitigating the risks of dual-use technology. Therefore, according to Elisa D. Harris, the objectives of dual-use technology governance can be conceptualized as general, such as nonproliferation, security, and safety. Alternatively, these governance objectives can be focused on more specific goals, including:

1. Prevent dual-use technologies from being developed and used for hostile purposes;
2. Control access to materials, equipment, and information or knowledge related to dual-use technology; and
3. Promote the safe and secure handling and use of materials, equipment, or information related to dual-use technology.

6.1. Palestine as a Laboratory for Dual-use Technology and Its Relevance in the Indonesian Context: Political Practices of Human Rights Misappropriation

Charles Santiago, co-chair of the ASEAN Parliamentarians for Human Rights (APHR), criticized the purchase and use of highly invasive spyware by an Israeli-based surveillance company to spy on critical groups expressing their freedom of expression. Santiago further noted the gap between their public claims and actual acts of repression:[220]

> "We are deeply shocked that despite the Indonesian government's long-standing support for the Palestinian people, they have purchased and used spyware that has been used against human rights defenders and journalists in Palestine, as well as around the world,
>
> It is the height of hypocrisy to openly condemn Israel while at the same time covertly employing the Israeli regime's tactics against its own Indonesian citizens."

This statement indicates a state's practice of hypocrisy in fulfilling its human rights obligations. Hypocrisy, claiming to comply with regulations while actively violating them, is common in the international system, where rules are often complied with even when they are violated.[221] Kate Cronin-Furman coined the term quasi-compliance to describe behavior that is clearly motivated by pressure to comply with a rule but not undertaken with the intention of actually fulfilling the requirements of that rule. Quasi-compliance is a kind of one-way mechanism, setting a new floor for state performance on human rights obligations. In other words, while international human rights pressure can measurably influence the behavior of repressive states, it cannot induce compliance with international standards in the absence of domestic motivation to comply.[222]

The Indonesian government has not yet signed the global governance mechanism for commercial cyber intrusions, indicating a lack of political will to engage in efforts to combat spyware abuse. Indonesia was not present at the Pall Mall Process or the joint statement produced by the Third Summit of Democracies in Seoul, South Korea. The Third Summit for Democracies, held on March 18, 2024, in Seoul, with the theme Galvanizing Multi-Stakeholder Action to Combat the Misuse of Commercial Spyware, produced a joint statement on combating the proliferation and misuse of commercial spyware. The statement, originally announced in

[220] APHR, "Indonesia Must Halt the Import and Use of Highly Invasive Spyware."
[221] Kate Cronin-Furman, *Hypocrisy and Human Rights: Resisting Accountability for Mass Atrocities* (Ithaca, NY: Cornell University Press, 2022).
[222] Cronin-Furman, *Hypocrisy and Human Rights*.

March 2023, has now been signed by several countries, including the United States, Japan, South Korea, and Finland, which are also members of the Pall Mall Process. In February 2024, a separate multi-stakeholder dialogue was held, initially initiated by the United Kingdom and France, designed to combat the misuse and proliferation of commercial surveillance tools. This process emerged in response to growing concerns about the misuse of commercial spyware, such as the Pegasus spyware developed by Israel's NSO Group.[223] Despite the diverse group of countries involved, the Indonesian government has not joined the process or commented on its existence. The Indonesian government's absence reflects the domestic politics and global identity of the use of commercial spyware.[224]

Indonesia still places sovereignty as a key principle to demonstrate the implementation of foreign and domestic policies as part of state autonomy. Efforts to maintain domestic policy space to pursue security, economic, and development goals are an important goal of diplomatic efforts. Although the Indonesian government engages with formal and informal governance mechanisms in the areas of cyber and critical technology, its approval is not automatic but is based on domestic concerns and specific geopolitical contexts. Indonesia has a relatively high global standing and material capabilities to resist pressure to join governance mechanisms.[225]

There are three factors underlying why the Indonesian Government still lacks political will and appears to be distancing itself from the Pall Mall Process and spyware diplomacy:[226]

1. Joining the Pall Mall Process may not be an immediate or appropriate diplomatic priority for the Indonesian government. Efforts to combat spyware are certainly not high on Indonesia's diplomatic agenda. In recent years, Indonesia's cyber diplomacy has largely focused on combating online terrorism, advocating for technological neutrality and data sovereignty, and calling for greater support for cyber capacity building in the Global South. Although cyber surveillance has emerged as a national security issue since the 2013 Edward Snowden revelations, it has not been prominent on the diplomatic agenda;
2. There is a more substantial argument, as Indonesia is suspected of using spyware in domestic and international cyber operations. This is a factor that has prevented Indonesia from taking a clear position on limiting the intrusive capabilities of commercial spyware. Indonesian authorities are suspected of using commercial spyware to spy on opposition leaders and activists;[227]
3. From a moral perspective, the Indonesian government does not view surveillance for national security purposes as an illegitimate state action. Indonesian government policy products, both legislation and regulations, prioritize development or internal security issues over countering surveillance. This policy direction demonstrates the Indonesian government's desire to maintain China's continued presence as Indonesia's technological perimeter despite strategic distrust between the two countries.

This suggests that the scope of many surveillance systems follows a clear trajectory: first, they serve as a means to control the people of the Global South through war and abusive border controls. Second, they serve to suppress dissent domestically against those who speak out against policies. Take, for example, General Atomics' MQ-9 Predator/Reaper (surveillance and

[223] The revelations of the Pegasus scandal and other misuse of commercial spyware have sparked strong reactions from governments and industry, including through the Pall Mall Process. To date, the process includes representatives from the African Union, Australia, the Gulf Cooperation Council, Malaysia, Japan, Singapore, the US, and Switzerland. Gatra Priyandita and Arindrajit Basu, "Why Haven't India and Indonesia Signed Up for Anti-Spyware Dialogue?" Royal United Services Institute, April 10, 2024, https://www.rusi.org/explore-our-research/publications/commentary/why-havent-india-and-indonesia-signed-anti-spyware-dialogue.
[224] Priyandita and Basu, "Why Haven't India and Indonesia Signed Up for Anti-Spyware Dialogue."
[225] Priyandita and Basu, "Why Haven't India and Indonesia Signed Up for Anti-Spyware Dialogue."
[226] Priyandita and Basu, "Why Haven't India and Indonesia Signed Up for Anti-Spyware Dialogue."
[227] See Amnesty International, *A Web of Surveillance*.

attack) drones. Their mission has expanded from military to US border surveillance, and finally to domestic surveillance of those opposing Immigration and Customs Enforcement (ICE), although they were also used in 2020 to spy on protesters following the murder of George Floyd. Other examples of military technology used against domestic populations include the battlefield-tested X10 drones from US startup Skydio, which have been deployed domestically to monitor those organizing against ICE, the Israeli genocide, and the Trump administration. In Europe, the Greek Coast Guard reportedly used its stock of Israeli-made Heron military drones (manufactured by Israel Aerospace Industries) to disrupt the Gaza Freedom Flotilla mission as it attempted to deliver aid to the Gaza Strip.[228]

Greg Grandin argues that Washington has traditionally viewed Latin America as a lab or training ground where the United States could regroup during periods of retrenchment and test new ways to control its neighbors.[229] Meanwhile, Palestine has become a lab for Israel, which places Palestine on its doorstep, providing millions of oppressed people with a laboratory for the most precise and successful methods of domination. Israel's role as an ideal ethnonationalist model depends on its ability to commercialize this message. While some countries want Israeli weapons or technology only to spy or disrupt dissident behavior and have no interest in building their own ethnoreligious entities, many others believe the myth of Israeli racial supremacy and want to emulate it in their own countries. Israel's defense industry is immoral because that is how it grew. Israel will sell to anyone except official enemies like North Korea, Iran, or Syria. [230]

Today, the population of Gaza is subjected to a coercive control experiment where the latest technologies and techniques are tested. The Palestinian laboratory can only thrive if enough countries believe in its basic premise. It is not surprising that repressive regimes want to emulate Israel's oppression, using Israeli technology to oppress their own undesirable or rebellious populations.[231] Palestine, Israel's laboratory, is thriving amidst global disruption and violence. The worsening climate crisis will benefit Israel's defense sector in the future, while countries are not responding with active measures to mitigate the impact of rising temperatures. In practical terms, this means higher walls and tighter borders, stricter refugee surveillance, facial recognition, drones, smart fences, and biometric databases. By 2025, the border surveillance industrial complex is estimated to be worth US$68 billion, and Israeli companies like Elbit are guaranteed to be among the primary beneficiaries.[232]

In 2020, the UN Human Rights Council released a list of companies, both local and foreign, operating in illegal settlements in the West Bank and East Jerusalem. The list included Airbnb, Booking.com, Expedia, JCB, TripAdvisor, and Motorola Solutions. None of these companies stopped operating there due to a lack of public or political pressure to do so.[233]

---

[228] Corporate Watch, "What's Driving the Militarization of Tech."

[229] Greg Grandin, Pulitzer Prize-winning historian, in his landmark 2006 book, Em*pire's Workshop: Latin America, the United States, and the Making of an Imperial Republic*. See Antony Loewenstein, *The Palestine Laboratory: How Israel Exports the Technology of Occupation Around the World* (London: Verso, 2023).

[230] Loewenstein, *The Palestine Laboratory*.

[231] Israel yearns for Western approval to fully realize its diplomatic and military potential. Besides the United States, Germany is arguably the greatest prize of all. Israel helps Germany repair its shattered image after World War II, while Berlin lends legitimacy to a state that brutally occupied Palestine, considered a non-people in the eyes of the German government. Germany's purchase of ever-increasing quantities of Israeli defense hardware is just one way to atone for its historical guilt. See Loewenstein, *The Palestine Laboratory*.

[232] Loewenstein, *The Palestine Laboratory*.

[233] A growing number of institutional investors are withdrawing investments from Israeli companies, citing concerns about complicity in Israeli human rights abuses. KLP, Norway's largest pension fund with US$95 billion in assets, withdrew investments from sixteen companies in 2021 due to their unacceptable risk of contributing to human rights abuses in West Bank settlements. In the same year, the New Zealand Super Fund sold US$6.5 million of its holdings in five Israeli banks, citing credible evidence that the companies involved provided project financing for illegal Israeli settlement construction. The tide may be turning. In 2021, the Responsible Investor website found that 67 percent of

The report of the Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967, Francesca Albanese, reinforces the fact that dual-use technology is evident in the Israeli occupation of Palestine. She states that civilian technology has long served as a dual-use tool of settler colonial occupation. Israeli military operations rely heavily on devices from leading global manufacturers to displace Palestinians from their land, destroy homes, public buildings, agricultural land, roads, and other vital infrastructure. Since October 2023, these machines have been integral to the damage and destruction of 70 percent of buildings and 81 percent of agricultural land in Gaza.[234] Francesca Albanese further states in the report:[235]

> The repression of Palestinians is increasingly automated, with technology companies providing dual-use infrastructure to integrate mass data collection and surveillance, while taking advantage of the unique testing ground for military technology offered by the occupied Palestinian territories. Driven by US technology giants establishing subsidiaries and research and development centers in Israel, Israel's claim of security needs has fueled an unprecedented development of detention and surveillance services, ranging from closed-circuit television (CCTV) networks, biometric surveillance, high-tech checkpoint networks, "smart walls" and drone surveillance to cloud computing, artificial intelligence and data analytics supporting military personnel in the field.

The report also identified the development of artificial intelligence systems developed by the Israeli military, such as "Lavender," "Gospel," and "Where's Daddy?". The technology is used to process data and generate target lists. These technological developments have transformed modern warfare and illustrate the dual-use nature of artificial intelligence.[236]

Special Rapporteur Francesca Albanese argues that Israel's economy of occupation has transformed into an economy of genocide, a transformation supported not only by the state but also by global technology companies. The report highlights how companies providing cloud infrastructure, artificial intelligence systems, and data analytics to Israel's military and intelligence services have become integral components of Israeli policy of expulsion and destruction.[237] Sara Roy describes this process in the current digital era as a colonial digital-military complex supported by the active participation of global corporations. This process reveals that digital colonialism functions not merely as a technical or economic phenomenon, but as a form of internationally legitimized domination. Israel's digital colonial order over Palestine is built on three fundamental layers: infrastructure, surveillance, and narrative.[238]

Companies like Palantir Technologies, through their artificial intelligence tools that provide precision targeting, have killed civilians en masse and transformed warfare into a planned and systematic campaign of extermination with little human oversight. The tech giant's involvement in Israel predates its formal agreement by years. Palantir has been active in Israel since 2015, the

---

fund managers thought human rights would soon become a key investment consideration, not unlike the centrality of climate change today. See, Loewenstein, *The Palestine Laboratory*.

[234] Albanese, *From Economy of Occupation to Economy of Genocide*.

[235] Albanese, *From Economy of Occupation to Economy of Genocide*.

[236] Palantir has provided automated predictive policing technology, core defense infrastructure for rapid, large-scale military software development and deployment, and an Artificial Intelligence Platform that enables real-time battlefield data integration for automated decision-making. In January 2024, Palantir announced a new strategic partnership with Israel and held a board meeting in Tel Aviv in solidarity. In April 2025, Palantir's CEO responded to accusations that Palantir had killed Palestinians in Gaza by saying, "mostly terrorists, that's true. This demonstrates executive-level knowledge and intent regarding Israel's unlawful use of force and failure to prevent such actions or withdraw complicity." See Albanese, *From Economy of Occupation to Economy of Genocide*.

[237] Diyar Saraçoğlu, "From Productive Force to Destructive Force: Digital Colonialism in Palestine," bianet, 7October2025, https://bianet.org/yazi/from-productive-force-to-destructive-force-digital-colonialism-in-palestine-312332.

[238] Saraçoğlu, "From Productive Force to Destructive Force."

time of a strategic agreement, called the Partnership for Battle Tech. Palantir's deep involvement in Israel's military infrastructure is part of a broader and worrying pattern of technology enabling warfare. That relationship extends to another tech giant – SpaceX's Starlink, led by Elon Musk. Understanding this complex relationship is crucial to understanding how modern conflicts are increasingly driven by advanced technologies developed by private companies.[239]

In late 2021, Microsoft CEO Satya Nadella met with the commander of Israel's military surveillance agency Unit 8200. The meeting focused on moving a large amount of classified intelligence to the US company's cloud. Intelligence chief Yossi Sariel secured Nadella's support for a plan that would give Unit 8200 access to a dedicated, segregated area within Microsoft's Azure cloud platform.[240] The use of the system has escalated during the Gaza campaign and has killed more than 60,000 people in the territory, most of them civilians, including more than 18,000 children. The company's engagement with Unit 8200 is based on strengthening cybersecurity and protecting Israel from state and terrorist cyberattacks.[241] This followed an investigation published by the Guardian that revealed how Azure was being used to store and process vast amounts of Palestinian communications in a mass surveillance program. Microsoft has cut off the Israeli military's access to the technology it uses to operate a sophisticated surveillance system that collects millions of daily Palestinian civilian phone calls in Gaza and the West Bank, as revealed by the Guardian. Microsoft stated on August 15, 2025, that Unit 8200, Israel's elite military spy agency, had violated the company's terms of service by storing vast amounts of surveillance data on its Azure cloud platform.[242] Microsoft's termination of services was based on the company's principles of (1) not providing technology to facilitate mass surveillance of civilians; and (2) respecting and protecting customers' privacy rights.[243]

In this regard, the military-industrial digital complex in the Israeli occupation of Palestine, the role of universities is significant as an integral part of the apparatus of oppression. Universities' involvement and responsibility in perpetuating the apartheid regime and in producing knowledge, technology, and narratives that serve the occupation. The science and technology departments of several universities serve as research and development centers for collaboration between the Israeli military and weapons contractors, including Elbit Systems, IAI, IBM, and Lockheed Martin, thus contributing to the production of tools for surveillance, crowd control, urban warfare, facial recognition, and targeted killing—digital technology tools that are effectively tested on Palestinians.[244]

---

[239] Business & Human Rights Resource Center, "Palantir & Starlink Allegedly Complicit in War Crimes amid Israel's War on Gaza," June 6, 2024, https://www.business-humanrights.org/en/latest-news/palantir-spacex-allegedly-complicit-in-war-crimes-amid-israels-war-in-gaza/.

[240] With Azure's nearly limitless storage capacity, Unit 8200 began building a powerful new mass surveillance tool: a vast and invasive system that collects and stores recordings of millions of mobile phone calls made daily by Palestinians in Gaza and the West Bank. Harry Davies and Yuval Abraham, "'A Million Calls an Hour': Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians," The Guardian, August 6, 2025, https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud

[241] Davies and Abraham, "'A Million Calls an Hour': Israel Relying on Microsoft Cloud."

[242] Davies and Abraham, "'A Million Calls an Hour': Israel Relying on Microsoft Cloud."

[243] See communication between Amnesty International and Microsoft Israel/IOPT in Amnesty International, "Microsoft's Move to Block Israeli Military Unit's Access to Its Mass Surveillance Technology Is a Moment for Corporate Reckoning," September 26, 2025, https://www.amnesty.org/en/latest/news/2025/09/microsoft-block-israel-military-unit-from-using-its-technology/.

[244] The Massachusetts Institute of Technology (MIT) conducts weapons and surveillance research funded by the Israeli Ministry of Defense. Israeli Ministry of Defense projects include drone swarm control, a distinctive feature of Israel's offensive in Gaza since October 2023, pursuit algorithms, and underwater surveillance. From 2019 to 2024, MIT managed the Lockheed Martin Seed Fund, which connected students with teams in Israel. From 2017 to 2025, Elbit Systems paid for membership in MIT's Industrial Liaison Program, allowing access to research and talent. In addition, the European Commission's Horizon Europe Program actively facilitates collaboration with Israeli institutions, including those implicated in apartheid and genocide. Since 2014, the European Commission has awarded more than €2.12 billion ($2.4 billion) to Israeli entities, including the Ministry of Defense, while European academic institutions

Israel also uses social media as a military tool as part of the chronicle of Israel's military occupation of the Palestinian territories and how social networks play a role as agents and mediators in this relationship. The intersection is between social media and militarism, between ordinary networking practices and wartime violence, between the pleasure of commonplace digital acts and the brutality of Israel's military occupation.[245] Adi Kuntsman and Rebecca L. Stein call this phenomenon digital militarism which:

> Describes the process by which digital communication platforms and consumer practices, during the first two decades of the 21st century, became military tools in the hands of state and non-state actors, both in the field of military operations and in the civilian framework.

In examining the meaning of digital militarism, the military occupation of the digital realm becomes the manifestation of dual-use technological devices in the context of the militarization of technology.

In general, according to Adi Kuntsman and Rebecca L. Stein, the digital of digital militarism is a highly diverse domain of new technologies and technological capabilities, including high-tech weaponry and cyber warfare, and Israel prides itself on its preeminence in mastering the militarization of technology. During the Israeli occupation, the role of social media and mobile technologies was instrumental in the way the state mobilized social media and mobile technologies and the connected public as tools, sites, and languages of military engagement. Therefore, the term digital militarism refers to the expansion of military culture into the domain of social media, often considered beyond the reach of state violence, and to the impact of militarization on everyday social networks in Israel. In the context of the Israeli occupation, these

---

benefit from and strengthen this engagement. The Technical University of Munich (TUM) received €198.5 million ($218 million) in funding from the European Commission's Horizon program, including €11.47 million ($12.6 million) for 22 collaborations with Israeli partners, military and technology companies. TUM and Israel Aerospace Industries (IAI) received €792,795.75 ($868,416) to jointly develop green hydrogen refueling, a technology relevant to IAI's military drones used in Gaza. TUM partners with IBM Israel – which manages Israel's discriminatory Population Registry – on cloud systems and artificial intelligence as part of IBM Israel's €7.02 million ($7.71 million) Horizon funding. TUM is also collaborating on a €10.76 million ($11.71 million) project called seamless urban mobility that encompasses the City of Jerusalem, a city that reinforces annexation through urban transportation. It is impossible to separate the expertise contributed by Israeli partners to these partnerships from the expertise acquired and used in the violations associated with them. Furthermore, many universities have maintained ties with Israel despite the post-October 2023 escalation. In one of many UK examples, the University of Edinburgh holds nearly £25.5 million ($31.72 million) (2.5 percent of its endowment) in four tech giants – Alphabet, Amazon, Microsoft, and IBM – that are central to Israel's surveillance apparatus and the ongoing destruction of Gaza. With direct and indexed investments, the university is among the UK's most financially entangled institutions. It also partners with companies that aid Israeli military operations, including Leonardo SpA and Ben Gurion University through its Artificial Intelligence and Data Science Laboratory, sharing research directly linking them to attacks on Palestinians. See Albanese, *From Economy of Occupation to Economy of Genocide*.

[245] During the waiting period for the attack, Israeli soldiers uploaded a series of selfies to their personal Instagram accounts. The standard catalog of smartphone self-portraits, including casual photos of young uniformed military personnel smiling into the camera, fits Instagram's investment in the beauty of the ordinary, showcasing everyday moments of uniformed military life, such as riding a bus, posing for a self-portrait in an elevator, hugging a friend, all framed by the temporality of the long wait, waiting to be deployed. With the help of retro filters and aesthetics, these mobile photos produce a beautiful and highly sanitized visual archive of military life. In doing so, they offer a digital touchstone to a long history of Israeli nationalist sentiment and associated iconography, in which war is simultaneously glorified and aestheticized while being divorced from the violence it causes. The Israeli military mobilizes through the selfie genre, an iconography that serves the needs of self-image, with war configured as a meme and used as a tool for micro-celebrity. These photos of militarism but not combat, of beautified bodies free of dirt or blood, are a considerable distance from the carnage of the military operations that occur simultaneously. The accompanying hashtags hint at a violence that has been sanitized by the visual field. When read together, the selfie and its accompanying hashtags produce a disturbing intersection of patriotism and intimacy, lethality and playfulness, soldiers and algorithms. See Adi Kuntsman and Rebecca L. Stein, *Digital Militarism: Israel's Occupation in the Social Media Age* (Redwood City: Stanford University Press, 2015).

two terms mutually shape each other: that is, the evolving use of social media impacts the field of Israeli militarism, just as shifts in Israeli militarization transform the field of social media.[246]

Digital militarism as a public relations strategy systematically demonstrates the diverse and often mundane ways in which the Israeli military regime and its pervasive culture of militarism are maintained and perpetuated. The militarization of social media is by no means unique to the Israeli context. Rather, as is now common knowledge, social media has been integrated into military operations in various contexts around the world, with platforms such as Twitter, Instagram, and YouTube being used as wartime public relations strategies, as surveillance and counterinsurgency tools, and as archives of perpetrator violence. In the social media era, contemporary warfare and armed conflict increasingly embrace digital communication platforms as a process that has expanded the theater of military operations and transformed users' understanding of the political functions and purposes of digital technologies.[247]

When Israel launched Operation Pillar of Defense in November 2012, it used social media platforms for the first time as an instrument of war. The expansion of Israel's military campaign into social media was not only driven by civilian users in various locations, both in Israel, Palestine, and the international arena, but also by the Israeli military's official social media unit. The military chose its own dedicated Twitter account to announce the start of operations, while they also prepared content on other platforms, such as YouTube, Flickr, Pinterest, and Facebook.[248]

The above illustration shows how Israel developed a world-class weapons industry by testing them on occupied Palestinians, then marketing them as "battle-tested." Leveraging the IDF brand has made Israeli security companies some of the most successful in the world. The Palestinian laboratory has become one of the selling points of Israeli weaponry. In fact, the Palestinian laboratory has been a state policy for almost the entire duration of the Israeli occupation of the Palestinian territories.[249] The Pegasus spyware produced by NSO[250] and Cellebrite causes damage worldwide, born of the history of Zionist militarism to develop the defense industry and then sell and promote it to the global market.[251] Ron Deibert argues that the main challenge to challenging the cyber surveillance industry is how to overcome the fact that the world today is run by a transnational class of gangsters. Therefore, without fundamental changes to the financial incentives inherent in companies like NSO, the future of the human condition is bleak. Surveillance of personal data and authoritarian state control have become

---

[246] Kuntsman and Stein, *Digital Militarism*.

[247] Kuntsman and Stein, *Digital Militarism*.

[248] The years after 2012 saw a substantial shift in the realm of Israeli digital militarism. In previous years, the military had primarily used the internet for counterinsurgency or as a broadcast medium for didactic messages. In 2012, the Israeli military used social media in a very different way. During the invasion, platforms like Facebook and Twitter became tools of war in their own right, transformed into so-called "warning technologies" and declarations of war. The contrast with the 2008–2009 campaign, according to many experts, was striking. From various media perspectives, the military was congratulated for the increased effectiveness, scale, and timeliness of its social media engagement. In Israel, as in many other geopolitical contexts, the militarization of the internet began in the form of hacking. Israeli online communities were first demilitarized on a large scale during the 2008–2009 military invasion of the Gaza Strip, codenamed Operation Cast Lead. The 2008–2009 Gaza invasion marked a milestone: the first official use of social media by the Israeli military. The need for a social media public relations strategy stems from the lessons of the second Lebanon war with Hezbollah in 2006, when the Israeli military was said to have lost the information battle due to various technological errors. See Kuntsman and Stein, *Digital Militarism*.

[249] Loewenstein, *The Palestine Laboratory*.

[250] The power of NSO and the state of Israel is nearly unstoppable, even ensnaring Apple, which was forced to issue an emergency software update in 2021 for its 1.65 billion users after Citizen Lab discovered a vulnerability in its operating system that had been exploited by NSO. Apple issued a press release directly alleging Israeli involvement. NSO Group creates sophisticated, state-sponsored surveillance technology that enables highly targeted spyware to monitor its victims. See Loewenstein, *The Palestine Laboratory*.

[251] Loewenstein, *The Palestine Laboratory*.

seemingly limitless and profitable business opportunities that undermine public accountability and facilitate despotic rule.[252]

The Indonesian government opposes Israel's actions against Palestine, and even today , the Indonesian government does not have diplomatic relations with Israel. However, at the same time, the Indonesian government continues to purchase spyware developed and tested on Palestinians. It is important to place Israeli spyware in the context that Palestine has become the perfect laboratory for the Israeli military-techno complex, encompassing surveillance, home demolitions, indefinite detention, and brutality, all the way to high-tech devices produced by start-up companies. Israel has become a global leader in spyware and defense hardware that fuels the world's most brutal conflicts. As ethno-nationalism grows in the 21st century, Israel has developed its ultimate model of new defense and surveillance technology to showcase to international investors and clients, including Indonesia.[253]

Israel and Indonesia do not have formal diplomatic relations, although discreet trade, tourism, and security contacts exist. In 2008, trade between Indonesia and Israel reached $900 million, with $300 million coming from coal. Trade between Jakarta and Tel Aviv reportedly reached $550 million in 2021, 84 percent of which were Indonesian exports. While Indonesia primarily exports commodities, Israel's exports primarily consist of high-tech products and cyber software.[254]

Israel is home to more spyware companies than any other country in the world, including NICE, Verint, NSO Group, Black Cube, Candiru, Cytrox, Cellebrite, and Intellexa. This spyware technology is designed and tested as part of the Israeli occupation and apartheid regime in Palestine. Once the technology is successfully tested, Israeli spyware companies are authorized by the Israeli Ministry of Defense to sell the technology for profit.[255] Of the 75 governments that have purchased spyware and digital forensics technology worldwide, 56 purchased from companies based in or connected to Israel, such as NSO Group, Cellebrite, Cytrox, and Candiru. All of these deals are monitored and approved by the Israeli Ministry of Defense. For Israel, spyware is not only a highly profitable industry but also a strategic weapon for gaining diplomatic favor. In addition to revolutionizing the world of espionage, the enormous demand for these tools is reshaping geopolitics, with Palestinian lives at the mercy of a nefarious global spyware game.[256] The country's spyware industry has benefited from the turnaround of intelligence officers, particularly Unit 8200. After spending their days monitoring every aspect of Palestinian life, they took that experience to the private sector to design and develop state-of-the-art surveillance devices and export them worldwide, to both democracies and dictatorships. Occupied Palestinians became guinea pigs as Israeli occupation weapons were developed and tested.[257] Several Israeli digital technology companies identified as being used in Indonesia are outlined below:

1. Cellebrite
   Cellebrite has sold its devices to Indonesia, even though they have been used to target political opponents and activists, including in West Papua and sexual minority groups.

[252] Loewenstein, *The Palestine Laboratory*.
[253] Loewenstein, *The Palestine Laboratory*.
[254] DIMSE, "Indonesia," https://dimse.info/indonesia/.
[255] War on Want, "Israeli Spyware Is Threatening Our Rights and Freedoms," https://waronwant.org/resources/israeli-spyware-threatening-our-rights-and-freedoms.
[256] According to a New York Times investigation, the NSO deal has played a central role in securing support from Arab states, including in the Abraham Accords negotiations, a 2020 diplomatic agreement normalizing relations between Israel and Arab states like Bahrain and the United Arab Emirates. As a result, companies like NSO Group can be seen as unofficial arms of the Israeli state, strengthening the country's military and diplomatic ties. See, New Internationalist, "How Palestine Became Israel's Spyware Test-Bed," https://newint.org/features/2023/10/02/spy-games.
[257] New Internationalist, "How Palestine Became Israel's Spyware Test-Bed."

Furthermore, Indonesia has used communications eavesdropping technology from the Israeli company Verint Systems to intercept communications from sexual minority communities.[258] During the genocidal attack on Gaza, Israel used Cellebrite devices to collect data from the mobile phones of thousands of Palestinians captured and abducted from Gaza. Although Israeli media claimed that all of these individuals were members of militant groups, the Israeli military later admitted that most were civilians. Cellebrite also received funding from the Pentagon's innovation unit to develop a product to map underground tunnels in the Gaza Strip.[259] In 2019, Cellebrite participated in the Annual Indonesia Security Summit in Jakarta, Indonesia. Indonesia's leading digital forensics company, Bounga Solusi Informatika, is the official provider of the Universal Forensic Extraction Device (UFED) in Indonesia. In 2019, CNN reported that the Indonesian police used Cellebrite technology to extract data from people accused of hate speech. The technology was also reportedly used to extract data from Indonesian activists. In 2020, Haaretz reported that Indonesia used Cellebrite technology to silence political dissent and to enforce controversial moral laws.[260]

2. Saito Tech, also known as Candiru
   Saito Tech is an Israeli cyber surveillance vendor that offers a cyber infiltration system, marketed under the name Cyrus. The technology is designed to infiltrate PCs, networks, and mobile devices, using exploits and deployment operations. According to a leaked Candiru commercial proposal from 2020, some of Candiru's capabilities compromise Windows PCs as well as Android and iOS mobile devices.[261] An Israeli software vendor registered as Saito Tech Ltd., Candiru is an Israeli company, so any sales constitute defense exports that require a license from the Israeli Ministry of Defense. The company is privately held, does not publish financial statements, and has changed its registered name four times. The company remains immovable, as it relies on three things it cannot control: (1) an Israeli export license; (2) an American fund purchasing its assets by 2025; and (3) a government willing to sign an agreement. Microsoft counts more than 100 victims, including politicians, journalists, academics, embassy workers, human rights activists, and political dissidents, and locates about half of them in Palestine. Avast reported in July 2022 that Candiru exploited a security flaw in Google Chrome against users in Lebanon, Turkey, Yemen, and Palestine. Subsequently, the Israeli Ministry of Defense reduced the list of countries to which Israeli companies could export offensive cyberware from 102 to 37, removing Saudi Arabia and the United Arab Emirates. Any Candiru sales are licensed based on that list, so the state of Israel, not the company, decides who can buy.[262] Amnesty International discovered shipments of hardware, which Amnesty International linked to the Candiru system, to the Indonesian National Police as the end user via Singapore-based Heha PTE Ltd (Heha).[263]
3. NSO Group

---

[258] New Internationalist, "How Palestine Became Israel's Spyware Test-Bed.". See also Amnesty International, *A Web Of Surveillance*.

[259] American Friends Service Committee, "Companies Profiting from the Gaza Genocide," https://afsc.org/gaza-genocide-companies.

[260] DIMSE, "Indonesia."

[261] Amnesty International, *A Web of Surveillance*.

[262] Stop Palestinian Genocide listed Saito Tech Ltd. (Candiru) as a priority campaign target because the company is considered to pose a high level of danger in the context of the Israeli occupation of Palestine and is quite vulnerable to campaign pressure. See, Stop Palestinian Genocide, "Candiru (Saito Tech Ltd)," https://palestiniangenocide.org/boycott/companies/candiru/.

[263] Although the shipment from Heha to the Indonesian National Police did not include any identifiable product or company name, Amnesty International cross-checked and found a significant correlation between the description and the delivery time indicating Candiru as the supplier of this cyber surveillance system. See, Amnesty International, *A Web of Surveillance*.

NSO Group is an Israel-based company that develops and sells the Pegasus spyware platform designed to covertly compromise mobile devices such as iPhones, Android devices, and Blackberries. Investigative group IndonesiaLeaks and its media partners, including Tempo, published an investigation in June 2023 identifying Indonesia as a potential customer for NSO Group's Pegasus spyware, which has been used to illegally target civil society members worldwide. IndonesiaLeaks' findings were based on an analysis of import records and statements from several anonymous sources indicating Pegasus was sold to, and used in, Indonesia. Furthermore, IndonesiaLeaks also reported that the Indonesian National Police and the State Intelligence Agency (BIN) had obtained access to Pegasus.[264] Each sale requires an export permit from the Israeli Ministry of Defense, so Israel decides who gets it. Citizen Lab, a research group at the University of Toronto, and Amnesty International's Security Lab independently confirmed the presence of Pegasus on the devices of six Palestinian human rights defenders on November 8, 2021. Israel had designated six Palestinian civil society organizations as terrorist organizations weeks earlier. Front Line Defenders argues that the designation is partly an attempt to legitimize the surveillance already conducted on its staff. A UN investigator, the Special Rapporteur on the occupied Palestinian territories, noted on June 30, 2025, that Pegasus had been used against Palestinian activists. Despite changing ownership to American investors, NSO Group says the investment does not remove the company from Israeli regulatory or operational control. Its headquarters and core operations remain in Israel, and it remains fully supervised and regulated by the Israeli Ministry of Defense. Any sales require a license from the Defense Export Control Agency, the ministry's export arm. The same UN report found that such exports enable spyware diplomacy while bolstering state impunity. NSO's defense is that its customers, not NSO, choose who to target.[265]

4. Wintego Systems Ltd (Wintego)
   Wintego is an Israeli cyber surveillance company that markets spyware for smartphones and various tactical network interception technologies under the WINT brand. Amnesty International identified network infrastructure associated with Wintego's Helios spyware, as well as malicious domains used in Indonesia and other countries. Amnesty International identified a Singapore-based Wintego reseller: Ataka Enterprises PTE Ltd (Ataka). Based on shipment data from commercial databases and information posted on websites and blog posts, Amnesty International has discovered information indicating that Wintego's cyber surveillance products were sold to the Indonesian National Police through two Singapore-based companies, Ataka and ESW System.[266]
5. Cognyte/Verint
   In 2018, Haaretz exposed the use of Verint products for improper surveillance of sexual and religious minority activists. In 2021, Verint spun off its cyber intelligence and defense divisions into an independent company called Cognyte. The new company continued its activities in Indonesia. In February 2022, Intelligence Online reported that Israeli firm Cognyte had secured a contract from the Indonesian intelligence agency;[267]
6. Corsight AI
   In 2021, Corsight AI announced its expansion into key regions in Asia, including Indonesia. In May 2021, Corsight AI partnered with Netpoleon, a Value-Added Distributor

[264] Amnesty International, *A Web of Surveillance*.
[265] Stop Palestinian Genocide listed Saito Tech Ltd. (Candiru) as a priority campaign target because the company was deemed to pose a high level of danger in the context of the Israeli occupation of Palestine and was quite vulnerable to campaign pressure. See Stop Palestinian Genocide, "NSO Group,"Stop the Palestinian Genocide, https://palestiniangenocide.org/boycott/companies/nso/.
[266] Amnesty International, *A Web of Surveillance*.
[267] DIMSE, "Indonesia."

(VAD) of Networking and Cybersecurity products headquartered in Singapore, to make facial recognition technology more accessible across Asia, including Indonesia.[268]

7. BriefCam
   According to official Company documents, BriefCam products are used by the Indonesian Police.[269]

The Indonesian government's use of spyware, which has been tested on Palestinians and is also used as part of state surveillance, is a manifestation of the misappropriation of human rights. At the Summit for a Peaceful Settlement of the Palestinian Question and the Implementation of the Two-State Solution, part of a series of UN General Assembly events, Prabowo delivered a speech calling for Palestinian independence:[270]

> "We must recognize Palestine now. We must stop the humanitarian catastrophe in Gaza... Ending the war must be our top priority. We must overcome hatred, fear, and suspicion. We must achieve the peace that humanity needs. With heavy hearts, we remember the unbearable and ongoing tragedy in Gaza. Thousands of innocent lives, many of them women and children, have been lost. Famine threatens. A humanitarian catastrophe is unfolding before our eyes."

Although President Prabowo Subianto condemned the ongoing Israeli attacks on Gaza, he failed to consider the Israeli weapon, Pegasus, which may still be operating domestically. Pegasus and other spyware are instruments of the Israeli occupation, then transformed into commercial instruments to be marketed as counterterrorism software. Through a network of intermediaries and local companies, Pegasus and other Israeli spyware products covertly surveil critical citizens. At this point, President Prabowo Subianto demonstrates the politics of human rights misappropriation, as he appears to be using human rights discourse to exclude or oppress certain groups and individuals while strengthening his authority.[271]

President Prabowo Subianto stands in solidarity with Gaza, but at the same time fails to dismantle Israel's digital footprint within the country. Pegasus is not just a product; it is part of the Israeli occupation economy. Pegasus has been refined through testing on Palestinians and then monetizing it globally. Pegasus carries the logic of occupation wherever it is marketed and traded: dissent is a threat, minorities are suspects, and critics are enemies.[272] Furthermore, President Prabowo Subianto's tendency to interpret human rights is clearly based on his idea, such as his use of the terms foreign stooges, black Dutchmen, treason perpetrators and terrorists which are aimed at individuals or collectives who criticize the government.

According to Tempo's analysis, the term "foreign stooge" is frequently used against government critics. The term "foreigner" has become increasingly common in response to demonstrations against President Prabowo Subianto's policies. In his speech on the 17th anniversary of the Gerindra Party and the commemoration of Pancasila Day, President Prabowo Subianto explicitly accused non-governmental organizations and media outlets of being paid by foreigners to destabilize Indonesia.[273]

---

[268] DIMSE, "Indonesia."
[269] DIMSE, "Indonesia."
[270] Deutsche Welle, "Points of Prabowo's Statement Regarding Palestine at the PPP Conference," https://www.dw.com/id/poin-poin-pernyataan-prabowo-soal-palestina-di-ktt-pbb/a-74102466.
[271] Gráinne de Búrca and Katharine G. Young, "The (Mis)appropriation of Human Rights," *Open Global Rights*, https://www.openglobalrights.org/misappropriation-human-rights/.
[272] Muhammad Zulfikar Rakhmat, "Indonesia Cannot Condemn Gaza Genocide While Still Silent on Its Use of Israeli Spyware," Middle East Monitor, September 30, 2025, https://www.middleeastmonitor.com/20250930-indonesia-cannot-condemn-gaza-genocide-while-still-silent-on-its-use-of-israeli-spyware/.
[273] BBC News Indonesia, "Aparat membungkam jurnalis dan aktivis dengan narasi antek asing, sebut laporan," 20 May 2026, https://www.bbc.com/indonesia/articles/cj4pqkw785lo.

However, at the same time, President Prabowo Subianto also uses the discourse of human rights and democracy, constructed within his own narrative. For example, in his inauguration speech, he stated his desire for a polite democracy typical of Indonesia, with minimal hostility and corrections without insults. This speech implied that President Prabowo Subianto's desire for polite democracy could be interpreted as prohibiting speech and protests in order to maintain public order. Ultimately, politeness in democracy is measured only through the eyes of those in power.[274]

President Prabowo Subianto then stated that he considered the implementation of human rights and Western-style democracy to be hypocritical. He then alluded to Western countries that preach democracy but continued to colonize Indonesia for hundreds of years. He also noted that Western countries often preach human rights but in practice also violate them.[275]

Prabowo's perspective can be interpreted as an attempt to re-examine the appropriateness of human rights and identify which human rights originate from the West and which are indigenous to Indonesia. Thus, this effort to re-examine the appropriateness of human rights will be accompanied by a rejection of the international human rights framework that has been canonized in the UN human rights system. This perspective appears to embrace human rights discourse and position itself as an authoritative interpreter of human rights with an Indonesian spirit. However, upon closer examination, rather than renewing the President's commitment to human rights, this Western-style human rights assignment is actually an attempt to appropriate human rights by changing the human rights canon from within, elevating certain human rights claimed to be Indonesian. A further consequence of this effort is that it will narrow human rights in accordance with conservative socio-political views to distinguish where human rights come from, who those rights protect most, and which rights are more important than others.[276]

Meanwhile, President Prabowo Subianto wants Indonesia to become a member of the Board of Board of Peace, initiated by US President Donald Trump.[277] Then, on November 17, 2025, the UN Security Council adopted Resolution 2803, known as the Board of Peace. The resolution called on all parties to implement Donald Trump's comprehensive plan and maintain the ceasefire in good faith and without delay. Paragraph 2 of the resolution described the Board of Peace as a transitional government with international legal personality that would govern the Gaza Strip until the Palestinian Authority completed its reforms as scheduled. It further stated that Palestinian self-determination and state sovereignty could be achieved only when the Palestinian Authority's reform program was completed and the reconstruction of the Gaza Strip was underway.[278]

---

[274] Tempo, "Demokrasi Santun Prabowo Subianto," October 23, 2024, https://www.tempo.co/kolom/demokrasi-santun-prabowo-subianto-1096274.

[275] Tempo "Natalius Pigai Respons Kritik Prabowo terhadap HAM Barat Hipokrit," December 9, 2025, https://www.tempo.co/hukum/natalius-pigai-respons-kritik-prabowo-terhadap-ham-barat-hipokrit-2097231.

[276] Jayne Huckerby, Sarah Knuckey, Appropriation and the rewriting of rights, *International Journal of Constitutional Law*, Volume 21, Issue 1, January 2023

[277] Trump's intention to establish the Board of Peace was evidenced in Executive Order 14375, which established the council as a public international organization. Similarly, the council's charter stipulates that the Board and its subsidiary entities will have international legal personality and will ensure the provision of the privileges and immunities necessary to carry out their functions. Previously, US Secretary of State Marco Rubio confirmed to members of the Senate that the board would have the same legal status as the United Nations. However, Marco Rubio later stated during his testimony before the Senate Foreign Relations Committee that the Donald Trump administration had decided to transform the Board of Peace from a public international organization composed of member states to an international nongovernmental organization (INGO). See Zaha Hassan, "Board Up Donald Trump's Failed Board of Peace," Carnegie Endowment for International Peace, June 17, 2026, https://carnegieendowment.org/middle-east/diwan/2026/06/board-up-trumps-failed-board-of-peace.

[278] Mohammad Yousef, "Why the Recent UNSC Resolution 2803 'Board of Peace' Violates the UN Charter," Middle East Monitor, November 21, 2025, https://www.middleeastmonitor.com/20251121-why-the-recent-unsc-resolution-2803-board-of-peace-violates-the-un-charter/.

This contradicts the principle of international law that the right of self-determination of the Palestinian people is an inalienable right enshrined in international law and cannot be subject to preconditions, such as reform of the Palestinian Authority and progress on the Gaza reconstruction plan.[279] Francesca Albanese supports this position, stating that:

> "The International Court of Justice (ICJ) has affirmed that self-determination is an inalienable right of the Palestinian people, and the United Nations and all states have an obligation to help realize it. This can only begin with the immediate and unconditional withdrawal of Israel's unlawful presence in the occupied Palestinian territory."

Meanwhile, according to the UN Special Rapporteur, the formation of the Board of Peace has no legal standing in international human rights law:[280]

> "As the aggressor and occupying power, this responsibility begins first and foremost with Israel and the countries that provide military and other support to its campaign in Gaza. The ceasefire must be maintained, the occupation must end, and guarantees must be made against its recurrence as a prerequisite for any sustainable, human rights-based reconstruction process. The formation of the Board of Peace is an illegal and illegitimate maneuver by powerful countries driven by nostalgia and greed."

However, President Prabowo Subianto sees it from a different perspective. Indonesia's presence presents an opportunity to achieve independence for Palestine. President Prabowo Subianto views membership in the Board of Peace as an effort to achieve peace in Gaza, Palestine. President Prabowo stated after signing the charter in Davos, Switzerland, on Thursday, January 22, 2026:[281]

> "I think this is a historic opportunity. This is truly an opportunity to achieve peace in Gaza. I have great hope, and Indonesia is ready to participate. Who wants peace there, who wants to help the people of Gaza, the Palestinian people?

---

[279] The recent advisory opinions of the International Court of Justice in 2024, all of which concluded that Israel's occupation of the Occupied Palestinian Territory (OPT), including the Gaza Strip, constitutes an illegal and aggressive occupation, calling for Israel to withdraw from all territories it occupied in 1967. Resolution 2803, meanwhile, does not mention Israel's occupation or call for its complete withdrawal. However, it does call on member states of the International Stabilization Forces (ISF) to work and cooperate with Israel. Israel, as an occupying power, cannot be treated as a neutral monitoring force and must cooperate with the Board of Peace to ensure the ceasefire is maintained. Furthermore, the Palestinian Authority and the Palestine Liberation Organization appear to have no role in the proposed plan; the resolution only mentions a newly trained and verified Palestinian police force without stating who and how they will be formed, and which Palestinian political body they will belong to. In other words, the resolution calls for legitimizing the Israeli occupation of the Gaza Strip and delegitimizing the Palestinian Authority, the Palestine Liberation Organization, and the right of self-determination of the Palestinian people. This violates Article 24(2) of the UN Charter, which states: "The Security Council shall act in accordance with the principles of the Charter." The UN Security Council acted beyond its authority by adopting Donald Trump's comprehensive plan that excludes the Palestinians and includes their occupiers. See, Yousef, "Why the Recent UNSC Resolution 2803 'Board of Peace' Violates the UN Charter."

[280] The UN human rights experts are (1) Balakrishnan Rajagopal, Special Rapporteur on adequate housing as a component of the right to an adequate standard of living, and on the right not to be discriminated against in this context; (2) Francesca Albanese, Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967; (3) Cecilia M. Bailliet, Independent Expert on human rights and international solidarity; (4) George Katrougalos, Independent Expert on the promotion of a democratic and just international order; (5) Paula Gaviria, Special Rapporteur on the human rights of internally displaced persons; (6) Pedro Arrojo-Agudo, Special Rapporteur on the human right to safe drinking water and sanitation; (7) Michael Fakhri, Special Rapporteur on the right to food; and (8) Margaret Satterthwaite, Special Rapporteur on the independence of judges and lawyers. See, Office of the United Nations High Commissioner for Human Rights (OHCHR), "UN Experts Condemn 'Board of Peace,' Call for a Reparative, Rights-Based Approach to Reconstruction in Gaza," https://www.ohchr.org/en/special-procedures/sr-housing/mr-balakrishnan-rajagopal.

[281] Tempo "Prabowo Ungkap Alasan Gabung Dewan Perdamaian Bentukan Trump," January 23, 2026, https://www.tempo.co/politik/prabowo-ungkap-alasan-gabung-dewan-perdamaian-bentukan-trump-2109216.

Prabowo even claimed that the situation in Gaza has improved following the Israeli aggression that began in 2023.

> "What is clear is that the suffering of the people of Gaza has decreased, significantly. Much reduced."

The establishment of the Board of Peace is important to place in the context of the Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967, Francesca Albanese. Her recent report, published on 20 October 2025, "Gaza Genocide: A Collective Crime," points out that the ongoing genocide against Palestinians must be understood as an internationally sanctioned crime. Many third countries have facilitated, legitimized, and ultimately normalized Israel's genocidal campaign. According to the Special Rapporteur, third countries have reproduced Israel's distortions of international law and colonial tropes, attempting to justify their own complicity in the genocide.[282]

The Special Rapporteur identified four interrelated components of the genocide of the Palestinian people in Gaza: diplomatic, military, economic, and humanitarian. These four components can be briefly described as follows: (1) genocide disguised as diplomatic and political action; (2) military relations providing the means of destruction; (3) weaponization of aid creating the conditions for genocide; and (4) economic and trade relations, particularly fuel and profits from the genocide. According to the Special Rapporteur, Indonesia has a role in diplomatic and political action,[283] particularly Indonesia's support for the establishment of the Board of Peace:[284]

> On September 30, 2025, many countries, including Egypt, Indonesia, Jordan, Pakistan, Qatar, Saudi Arabia, Turkey, and the United Arab Emirates, supported the Trump Plan even though it did not address ending the occupation, ensuring accountability, or providing transitional justice, and imposed foreign, imperial governance mechanisms on Gaza that would further undermine rather than realize the right to self-determination of the Palestinian people;

The report found that economic and trade ties also contributed to the genocide in Gaza. Transactions of spyware between Indonesia and Israel, even through third-party

---

[282] Francesca Albanese, *Report of the Special Rapporteur on the Situation of Human Rights in the Palestinian Territories Occupied since 1967: Gaza Genocide: A Collective Crime*, A/80/492 (New York: United Nations, 20 October 2025).

[283] Prolonged political and diplomatic support from influential third countries has enabled Israel to initiate and sustain its attacks on the Palestinian people. In the past two years, entrenched complicity characterized by manipulating narratives and reproducing Israeli lies has silenced urgent calls for action and obscured the intertwining of political, financial, and military interests. The long-standing failure to address Israel's gross violations of international law has normalized, deepened, and reinforced the oppression, domination, and erasure of the Palestinian people. See Albanese, *Gaza Genocide: A Collective Crime*.

[284] Several important points of the Joint Statement of the Foreign Ministers of Jordan, the United Arab Emirates, Indonesia, Pakistan, Turkey, Saudi Arabia, Qatar, and Egypt, as follows: 1) Welcoming the leadership of President Donald J. Trump and his sincere efforts to end the war in Gaza, and affirmed their confidence in his ability to find a path to peace. 2) Affirmed their willingness to engage positively and constructively with the United States and the parties to finalize the agreement and ensure its implementation, in a manner that ensures peace, security, and stability for the people of the region. 3) Reaffirmed their shared commitment to work with the United States to end the war in Gaza through a comprehensive agreement that ensures the delivery of sufficient humanitarian aid to Gaza without restrictions, no expulsions of Palestinians, the release of hostages, a security mechanism that ensures the security of all parties, a full Israeli withdrawal, the reconstruction of Gaza, and creating a path to a just peace based on a two-state solution, in which Gaza is fully integrated with the West Bank within a Palestinian state in accordance with international law as key to achieving regional stability and security. See, Ministry of Foreign Affairs of Pakistan, "Joint Statement by the Foreign Ministers of Jordan, United Arab Emirates, Indonesia, Pakistan, Türkiye, SaudiArabia, Qatar and Egypt," https://mofa.gov.pk/press-releases/joint-statement-by-the-foreign-ministers-of-jordan-united-arab-emirates-indonesia-pakistan-turkiye-saudi-arabia-qatar-and-egypt.

intermediaries in the dual-use technology supply chain, would strengthen Israel's capacity to produce dual-use technology. The Special Rapporteur's report stated:[285]

> Many Israeli imports are dual-use goods, which can be used in both civilian and military production. Often marketed as civilian technology, these dual-use goods are crucial to Israel's military system, which spies on, controls, and kills Palestinians, reinforcing the military-civilian economic symbiosis and the country's role in the global technological arms race.

The import of dual-use technology from Israel is framed through the views of Gráinne de Búrca and Katherine Young as a form of misappropriation of human rights. Misappropriation of human rights refers to the practice of using the language of human rights, but to serve exclusive, repressive, or anti-pluralist purposes.[286] In this regard, according to Kristina Stoeckl, the appropriation of rights is not something specific to a particular group of actors and ideological worldview, but rather, all meanings of human rights are constructed within concrete social and political practices. All actors involved in human rights actions and politics in one way or another make rights their own and imbue human rights provisions with contextualized meanings. Kristina Stoeckl further acknowledges that some human rights appropriations can have exclusionary and repressive effects, especially when they reinforce existing power imbalances and marginalize vulnerable people.[287]

7. The Intersection of the Rise of Militarization and the Use of Dual-use Technology: Identifying Its Impact on Human Rights

Although Indonesia has entered the democratic era in 1998, traces of active military involvement are still clearly visible. This military involvement aimed at encouraging voter participation was neither extraordinary nor coincidental. Rather, it was a response to the concerns of the then-incumbent president, Joko Widodo. According to President Joko Widodo's calculations, low voter turnout could threaten his re-election chances. The military's campaign paid off: voter turnout in the 2019 presidential election reached 79%, a figure significantly higher than the previous election in 2014 and even the highest since the introduction of direct presidential elections in 2004.[288] This demonstrates the new coalitional presidential system in Indonesia, which, according to Marcus Mietzner, allows the military to partially recover its power. This occurs because the military positions itself as a key element in the presidential coalition and capitalizes on the view of most presidents that excluding the military from the division of power would destabilize civilian rule. The coalitional presidential system demonstrates how civil military relations in Indonesia is greatly influenced by the special relationship that the president has with the political environment around him.[289]

---

[285] Albanese, *Gaza Genocide: A Collective Crime*.

[286] Gráinne de Búrca and Katharine G. Young, "The (Mis)appropriation of Human Rights by the New Global Right: An Introduction to the Symposium," *International Journal of Constitutional Law* 21, no. 1 (January 2023).

[287] Saskia Schäfer and Daniel Peterson, "Appropriations of Human Rights Discourses: Evidence from Indonesia and Malaysia," *International Journal of Constitutional Law* 24, no. 1 (January 2026).

[288] President Joko Widodo's circle has identified low voter turnout as the biggest threat to his re-election campaign. To that end, President Joko Widodo has taken systematic steps involving the military. Wiranto, as Coordinating Minister for Political, Legal, and Security Affairs, threatened in March 2019 that those who advocated abstention could be prosecuted under anti-terrorism laws. The military took similar action, launching a campaign to encourage voters to go to the polls. Posters distributed throughout Indonesia even featured images of the then-TNI Commander, Air Chief Marshal Hadi Tjahjanto, and the National Police Chief, General Tito Karnavian. See Marcus Mietzner, "The Military's Transformation from Praetorian Ruler to Presidential Coalition Partner," in *Oxford Research Encyclopedia of Politics*, ed. Erin Hannah (New York: Oxford University Press, 2020).

Under President Joko Widodo's administration in 2019, the military has solidified its political position as a key element in the presidential coalition. However, the military no longer has the means or authority to shape the political landscape, and its power fluctuates according to the dynamics of the presidential coalition, including both political parties and influential state actors. Nevertheless, the existing political dynamics demonstrate that the military's role remains politically relevant and has not experienced the depoliticization expected by civilian reformers following the 1998 regime change. This means that the military is now one of many actors in Indonesia's complex post-authoritarian political dynamics.[290] According to Muhammad Haripin, in response to the unstable political situation, President Joko Widodo adopted a political strategy by forging a political alliance with the military, and to some extent with the police. President Joko Widodo positioned the military's role as a countervailing force against pressure from the political opposition.[291]

The military's resurgence in politics, a manifestation of the ideas and practices of the New Order era, is inseparable from the role of Joko Widodo. Joko Widodo framed political practices with the characteristics of the New Order government, such as developmentalism, oppression, limited competition, weak accountability, and the centralization of state power. Joko Widodo is a figure who bears the main responsibility for the decline of democracy, including the strengthening of militarization that became the seeds of the growth of the New Order regime. According to Sana Jaffrey and Eve Warburton, there are two main characteristics of Joko Widodo's presidency: (1)the return of developmentalism in the economic sector; and (2) the rise of authoritarianism in the political sector.[292] The weakening of the Corruption Eradication Commission (KPK); the drafting of a new Criminal Code (KUHP) that makes criticism of public officials a criminal offense; and the Omnibus Law on Job Creation, which strips away worker protections and environmental protection provisions, reinforces the instillation of authoritarian patterns in political discourse and practice during Joko Widodo's leadership. Furthermore, Joko Widodo silenced opposition from civil society actors through systematic repression to narrow the space for legitimate dissent.[293] Ken Setiawan further stated that the Joko Widodo administration has weaponized online surveillance and intimidation to intimidate political opponents and stifle public criticism. Law Number 11 of 2008 concerning Electronic Information and Transactions (ICT Law) has been

[289] In addition to the coalitional presidential system, the driving factors for the politicization and depoliticization of the military in Indonesia are also influenced by three other patterns, namely: (1) the key role of the revolutionary period in strengthening the military's belief that it still has the right to have a political role, as well as in giving birth to the military doctrine that underlies this claim; (2) internal conflicts among civilians and other weaknesses in democratic politics that became factors that attracted the military's political activities, both in the mid-1950s, the 1960s, and during the immediate post-1998 transition period; and (3) the success of civilian politicians in maintaining general economic and political stability, such as in the early 1950s or after 2004, provided the best guarantee for curbing the military's political ambitions. See, Mietzner, "The Military's Transformation from Praetorian Ruler."

[290] Mietzner, "The Military's Transformation from Praetorian Ruler."

[291] Muhamad Haripin and Adhi Priamarizki, "Jokowi Consolidates Influence over TNI as Elections Loom," New Mandala, https://www.newmandala.org/jokowi-consolidates-influence-over-tni-as-elections-loom/.

[292] Sana Jaffrey and Eve Warburton, "Introduction: Jokowi's Decade in Power," in *The Jokowi Presidency: Indonesia's Decade of Authoritarian Revival*, ed. Sana Jaffrey and Eve Warburton (Singapore: ISEAS–Yusof Ishak Institute, 2025).

[293] Joko Widodo's intolerance of dissent has gained support from his allies in the House of Representatives and was formalized in 2022 as part of Indonesia's new Criminal Code, which contains harsh penalties, including imprisonment, for anyone criticizing public officials. One important factor that allows Joko Widodo to suppress civil society groups is related to the presence of the police force, which is under his influence. According to Sidney Jones, during Joko Widodo's ten-year administration, the police force has become almost an extension of his personal power. Furthermore, Sidney Jones shows that Joko Widodo has learned a lot about the importance of security actors, especially the police, as a political instrument to protect allies and intimidate opponents. For a populist figure, this requires efforts to stem political threats. Security actors become crucial allies in maintaining power. See, Jaffrey and Warburton, "Introduction: Jokowi's Decade in Power."

used to silence criticism from political opponents, journalists, activists, and ordinary citizens.[294] This demonstrates that Indonesia, like Russia,[295] is among the many countries that control the internet through legal and technical mechanisms. Like Russia, Indonesia has established laws and technical guidelines for years to control online information. The implementation of controls, such as content blocking, in Indonesia is decentralized. This means that while the government sets guidelines regarding what content should be blocked, the technical implementation is left to the discretion of each internet service provider. Legislative frameworks, such as the Law on Electronic Information and Transactions and the Law on Pornography, are often used as justification for internet control.[296] Technical approaches to internet control present challenges because, unlike legal frameworks that are more readily understood by the public, technical methods tend to be less clearly visible and requires specialized knowledge or expertise to understand. The implementation of controls through internet infrastructure or technical means impacts freedom of expression and access to information. Furthermore, as governments experiment with various technical methods to control the internet, there is potential to impede the flow of online information.[297]

The dramatic shrinkage of civil space during President Joko Widodo's administration is evident in the implementation of the Electronic Information and Transactions Law, which is one of the government's primary weapons to target its opponents. The government's misuse of the ITE Law appears to be yielding results. There is already clear evidence of a chilling effect within Indonesian society.[298]

State surveillance was strengthened through the establishment of the Cyber Unit by the Indonesian National Police in 2021 to expand the reach and capabilities of social media monitoring with the help of spyware. The government then further strengthened its surveillance capabilities through Ministerial Regulation No. 5 of 2020, which requires private digital services and platforms to register with the Ministry of Communication and Information Technology and submit personal user data to government agencies. This allows these tools to be used to monitor civil society activists and journalists.[299] Amnesty International's report reinforces state

[294] Ken MP Setiawan, "A State of Surveillance? Freedom of Expression under the Jokowi Presidency," in *Democracy in Indonesia: From Stagnation to Regression?* ed. Thomas Power and Eve Warburton (Singapore: ISEAS–Yusof Ishak Institute, 2020).

[295] Russia has passed a law that facilitates state-directed internet control while imposing technical obligations on information intermediaries. The country's internet regulator, Roskomnadzor, enforces this law and has issued a series of detailed technical recommendations for Internet Service Providers (ISPs) to filter or block online content. Non-compliance results in sanctions, such as fines. Internet control in Indonesia is not carried out by operating a nationwide technical filtering system like China's Great Firewall, but is instead left to internet service providers with the necessary technical capacity and capabilities. See Irene Poetranto, "Techno-Legal Internet Controls in Indonesia and Their Impact on Free Expression," in *Digital Democracy in a Divided Global Landscape* (Washington, DC: Carnegie Endowment for International Peace, 2025), 35–38.

[296] Poetranto, "Techno-Legal Internet Controls in Indonesia."

[297] Citizen Lab identified that by 2024, most internet service providers in Indonesia were implementing blocking using whatever methods they saw fit. One possible reason is that Domain Name System (DNS) redirection is more expensive and difficult for internet service providers to implement than other forms of DNS manipulation. Information intermediaries are often responsible for implementing internet controls, and have the technical mandate to block, monitor, or redirect internet traffic upon government request. See, Poetranto, "Techno-Legal Internet Controls in Indonesia."

[298] A 2022 survey conducted by Indikator Politik showed that 62.9 percent of Indonesians were afraid to express their opinions openly. Similarly, an October 2024 survey by Saiful Mujani Research and Consulting (SMRC) found that as President Joko Widodo's 10-year term drew to a close, 51 percent of respondents were afraid to discuss politics. This figure represents a significant increase compared to 2014, when Joko Widodo took office, when only 22 percent of Indonesians admitted to being afraid to discuss politics. See Tim Mann, "Activists on Trial: The Weaponization of Online Defamation Provisions in Indonesia," Australian Journal of Asian Law 25, no. 2 (2025): 1–16.

[299] Andreas Ufen, "The Rise of Digital Repression in Indonesia under Joko Widodo," *GIGA Focus Asia*, no. 1 (January 2024), https://doi.org/10.57671/gfas-24012.

surveillance efforts that threaten the freedoms and fundamental rights of citizens, particularly technology users:[300]

> The number of sales and distribution of highly invasive spyware identified in Indonesia is extremely worrying. On the other hand, civil space has shrunk in recent years due to ongoing attacks on the rights of freedom of expression, peaceful assembly and association, personal security, and freedom from arbitrary detention.

Furthermore, President Joko Widodo also utilized intelligence tools to make political parties, pillars of democracy, the objects and targets of surveillance. This action not only indicates abuse of power, but also undermines democracy, weakens the rule of law, and threatens human rights.[301] This use of intelligence data is a manifestation of President Joko Widodo's statement that he will interfere in the election under the pretext of being for the good of the nation. The use of intelligence data could be misused to support his electoral interests in the 2024 election, supporting the candidacy of Gibran Rakabuming Raka as Prabowo Subianto's running mate.[302]

According to Muhamad Haripin, President Joko Widodo's statement demonstrates a conflict of interest in the relationship between the president and intelligence agencies. President Joko Widodo is considered to be engaging in political espionage related to his statement claiming to possess intelligence data on the internal conditions and agendas of political parties. The misuse of intelligence data is inseparable from three fundamental problems related to the relationship between the president and intelligence agencies: regulatory weaknesses, conflicts of interest, and threat complexity. President Joko Widodo's statement that he possesses intelligence data on the internal conditions and agendas of political parties (parpol) demonstrates a conflict of interest in the relationship between the president and intelligence agencies.[303] The cyberattack targeting the Coordinating Minister for Economic Affairs, Airlangga Hartarto, which is suspected to be state-sponsored, can be seen in this context. An email message from Apple Inc. in November 2021 stated that Apple identified several individual officials as targets of state-sponsored attacks.[304] The use of state-sponsored spyware demonstrates the abuse of power by the president to exploit the capacity of intelligence agencies for the president's political interests.

Prabowo Subianto's election as president in the 2024 election marked the end of liberal democracy in Indonesia and the return of the New Order model of government. President Joko Widodo's dismantling of the pillars of liberal democracy in Indonesia facilitated the return of the dual function doctrine, a key pillar of the New Order, through amendments to the Law on State Civil Apparatus and the Law on the Indonesian National Armed Forces.[305] As a further

---

[300] Amnesty International, *A Web of Surveillance*.

[301] Tempo, "Jokowi Pamer Pegang Data Intelijen Arah Parpol, Begini Bunyi Pasal 1 dan 2 UU Nomor 17 Tahun 2011 tentang Intelijen Negara," September 20, 2023, https://www.tempo.co/politik/jokowi-pamer-pegang-data-intelijen-arah-parpol-begini-bunyi-pasal-1-dan-2-uu-nomor-17-tahun-2011-tentang-intelijen-negara-141871.

[302] Haripin and Priamarizki, "Jokowi Consolidates Influence over TNI."

[303] Aryo Putranto Saptohutomo, "Jokowi Dinilai Lakukan Intelijen Politik saat Kantongi 'Rahasia' Parpol," Kompas.com, September 22, 2023, https://nasional.kompas.com/read/2023/09/22/06000011/jokowi-dinilai-lakukan-intelijen-politik-saat-kantongi-rahasia-parpol?page=all.

[304] The attack targets included Chief Economic Minister Airlangga Hartarto, senior military personnel, two regional diplomats, and advisers at the Indonesian defense and foreign ministries. See, the attack targets included Chief Economic Minister Airlangga Hartarto, senior military personnel, two regional diplomats, and advisers at the Indonesian defense and foreign ministries., Reuters, "Indonesian Officials Targeted by Spyware: Sources," Al Jazeera, September 30, 2022, https://www.aljazeera.com/economy/2022/9/30/indonesian-officials-targeted-by-spyware-sources.

[305] Tim Lindsey, "Indonesia's New President, Prabowo Subianto, Finds Democracy 'Very Tiring'. Are Darker Days Ahead for the Country?" The Conversation, October 18, 2024, https://theconversation.com/indonesias-new-president-prabowo-subianto-finds-democracy-very-tiring-are-darker-days-ahead-for-the-country-241256.

consequence, President Prabowo Subianto began to revive the New Order era of praetorianism by expanding the capacity and reach of the military's political influence into civilian life. This is at least indicated by the inauguration of 162 new units, including six regional military commands (kodam), and the inauguration of several high-ranking officers by President Prabowo Subianto. The addition of new units and high-ranking officers is a follow-up to Presidential Regulation (Perpres) Number 84 of 2025, which revised Presidential Regulation No. 66/2019. The new Perpres regulates 420 high-ranking officer positions, an increase of 49 from the previous one. Regulations legalizing the placement of military officers in public office were strengthened through Law No. 3/2025 concerning Amendments to Law No. 34/2004 concerning the Indonesian National Armed Forces. President Prabowo Subianto intends to build territorial infrastructure that has the potential to become a channel for political influence down to the village level, repeating the military's role during the New Order era. According to Dwi Munthaha, President Prabowo Subianto's political moves are a manifestation of military praetorian-entrepreneurship, as the military is not only involved in politics but also controls business networks and public resources.[306]

The military praetorian-entrepreneur phenomenon can be seen in the implementation of MBG and the Red and White Cooperative. The TNI's implementation of MBG is evident, among other things, in the inauguration of 339 Nutrition Fulfillment Service Units (SPPG) by the TNI commander at Adi Soemarmo Air Force Base, Central Java, on September 26, 2025. With this inauguration, the total number of SPPGs under the TNI reached 452 units throughout Indonesia.[307]

At the same time, the TNI was also involved in implementing the red and white cooperative program through the signing of a cooperation agreement between PT Agrinas Pangan Nusantara and the TNI on October 10, 2025.[308] The agreement contained the military's authority to participate in accelerating the construction of cooperative buildings in the region. This involvement is also based on Circular Letter No. 4 of 2025 concerning Land and Building Asset Data Collection for the Acceleration of the Red and White Cooperative, issued by the Minister of Cooperatives. One point stipulates that village officials must coordinate with the local military district command to record assets in the form of land and buildings. The commander of the local unit will then report the asset data to PT Agrinas Pangan.[309]

Traces of military involvement in economic affairs were evident during President Suharto's leadership in the late 1960s and throughout much of the 1970s. This period represents a classic example of a praetorian state. The military dominated all branches of government, tightened its control over society, and intervened deeply in the Indonesian economy.[310] This new instrumentation and infrastructure of the TNI's political and economic influence was further strengthened through the expansion of the TNI's authority to engage in matters beyond defense (military operations other than war) and into the cyber realm.[311]

---

[306] Dwi Munthaha, "Militer Era Prabowo: Pretorianisme Baru?" *Kompas.id*, August 20, 2025, https://www.kompas.id/artikel/militer-era-prabowo-pretorianisme-baru.

[307] Indonesian National Armed Forces (TNI) Army Chief of Staff General Maruli Simanjuntak explained that the reason for the TNI's extensive involvement in the MBG Program was driven by the need to strengthen the program's social and economic impact. See Tempo, "KSAD Jelaskan Alasan TNI Banyak Terlibat dalam Program MBG," November 10, 2025, https://www.tempo.co/politik/ksad-jelaskan-alasan-tni-banyak-terlibat-dalam-program-mbg-2087989.

[308] Tempo, "Koperasi Desa Merah Putih," *Tempo.co*, https://www.tempo.co/tag/koperasi-desa-merah-putih.

[309] Tempo, "Cerita Kepala Desa soal Peran Tentara di Kopdes Merah Putih," February 16, 2026, https://www.tempo.co/politik/cerita-kepala-desa-soal-peran-tentara-di-kopdes-merah-putih-2115459.

[310] Mietzner, "The Military's Transformation from Praetorian Ruler."

[311] There is global expectation that the military, including the Indonesian National Armed Forces (TNI), will be able to carry out diverse roles beyond conventional warfare against foreign enemies and counter-insurgency missions. This expanded role presents complex challenges. Unlike conventional warfare or interstate armed conflict, the success of peacekeeping or stability missions, humanitarian and disaster relief missions, and counter-terrorism operations is

Law Number 3 of 2025 concerning Amendments to Law Number 34 of 2004 concerning the Indonesian National Armed Forces (TNI) substantively contains significant changes, including an expansion of authority. According to Muhammad Haripin, the significance of the revision of the TNI Law can be seen in several dimensions:[312]

First, the revision of the Law on the TNI allows for the expansion of TNI military operations other than war, by adding two additional missions, namely cyber defense missions and protecting Indonesian citizens and national interests abroad;[313]

Second, the revised Law on the TNI stipulates that active military officers can be appointed to five ministries and non-defense state institutions, including the National Border Management Agency (BNPP), the National Disaster Management Agency (BNPB), the National Counterterrorism Agency (BNPT), the Maritime Security Agency (Bakamla), and the Attorney General's Office (Kejaksaan Agung);

Third, the TNI's authority to formulate national defense policies and strategies is implemented in coordination with the Ministry of Defense. This means that the military headquarters has become relatively equal to the Ministry of Defense. Consequently, the TNI's increased autonomy in strategic matters will likely reduce civilian control over military matters through the ministry.

These significant changes have indeed fundamentally altered Law No. 34/2004 concerning the Indonesian National Armed Forces (TNI). This law expressly prohibits military involvement in politics, business activities, and other political appointments. According to the provisions of this law, military operations other than war are divided into 14 types of operations, including counter-insurgency, counter-terrorism, disaster relief, border security, peacekeeping, and military assistance to local governments and the police. This law requires that all military operations other than war require a state political decision from the president and the legislature, which serves as a framework to ensure legality, operational clarity, and resource allocation while maintaining civilian oversight.[314]

Since President Prabowo's inauguration, Indonesia's defense modernization efforts appear to have accelerated significantly. In January 2025, the Indonesian Ministry of Defense announced plans to nearly double the defense budget, setting a target of 1.5% of Indonesia's gross domestic product (GDP), compared to the previous 0.8% of GDP allocated to the military. While the budget increase appears to signal a serious commitment to military expansion, Indonesia appears to be aggressively purchasing to fill pressing defense gaps, lacking a unified strategy for military cohesion and interoperability. Efforts at military cooperation with various powers, including China, the United States, Russia, South Korea, Japan, and Australia, are at risk of weakening

difficult to measure. See Muhamad Haripin, *Civil-Military Relations in Indonesia: The Politics of Military Operations Other Than War* (Abingdon: Routledge, 2020).

[312] The revision also extends the retirement age for military personnel, which will disrupt the personnel regeneration cycle, thus causing an imbalance in the military hierarchy pyramid structure. See, Muhamad Haripin, "Indonesian Parliament Passes Law Expanding Military's Role in Government," *ADRNI Issue Briefing*, April 17, 2025, http://adrnresearch.org/publications/list.php?cid=2&idx=407&ckattempt=3.

[313] The basic idea of military operations other than war is based on the need for a new, collaborative and more resilient approach to address contemporary security challenges, such as terrorism, transnational crime, such as drug, arms, and human trafficking, piracy, and separatist movements. Based on this background, limiting the military's function to only conventional combat against foreign invasion or interstate war is considered irrational. This idea was further institutionalized through Law Number 34 of 2004 concerning the Indonesian National Armed Forces (TNI). This law stipulates that the Indonesian military has two primary functions: military operations and Military Operations Other Than War. See Haripin, *Civil-Military Relations in Indonesia*.

[314] Diandra Megaputri Mengko and Aulia Fitri Rosadi, "Non-Institutionalized Civilian Control and Military Operations Other than War in Indonesia," in *Military Modernization and Civil-Military Relations in Indonesia*, ed. Muhamad Haripin, Adhi Priamarizki, and Leonard C. Sebastian (Singapore: Palgrave Macmillan, 2025).

Indonesia's strategic autonomy, which actually places Indonesia in the midst of competing geopolitical interests.[315]

TNI modernization efforts began at least in 2009 under the Minimum Essential Force (MEF) scheme. This scheme was designed to improve three sectors: deployment capability, increased strike power, and enhanced military operations capabilities other than war.[316]

Weapons modernization in Indonesia refers to the General Defense Policy Guidelines stipulated by Presidential Regulation of the Republic of Indonesia Number 111 of 2025 concerning the General State Defense Policy for 2025-2029. This regulation identifies hybrid threats to Indonesia, including integrated cyber attacks, drone attacks, abuse of artificial intelligence, disruption of Command Control, Communication Computers, Cyber-Defense, Combat System Intelligence, Surveillance and Reconnaissance (C6ISR).[317] The use of dual-use technology can refer to the direction of the Defense Technology and Industrial Capability Development Policy, including:[318]

1. Development of defense technology capabilities is directed at: (1) mastery of key technology for priority programs that have a design, namely radar, military satellites, unmanned weapons systems (aircraft/surface vessels/underwater vessels/unmanned vehicles), and/or underwater sensing; (2) development of technological capabilities supporting strike power, mobility, sensing, or electronic and cyber warfare; (3) development of computer and network-based information and communication technology capabilities by paying attention to the interoperability of command and control systems; (4) development of communication system capabilities, navigation, remote sensing, and military satellite-based intelligence; (5) utilization of Artificial Intelligence, large data sets (big data), machine learning, automation systems, and robot technology for the benefit of National Defense;
2. Development of technological support capabilities and defense industry is directed at (3) strengthening the raw materials and strategic components industry as well as industries that utilize dual-use technology (multipurpose for civil/military purposes) which has a multiplier effect on strengthening the national industry.

Weapons modernization in Indonesia is developed through the concept of triple helix cooperation. This model is expected to generate greater economic impact than simply acquiring

[315] There are still gaps in the cohesion of Indonesia's procurement strategy, reflected in the diverse range of countries from which it purchases weapons. In June 2025, Indonesia completed the acquisition of TF KAAN fighter jets made by Turkish Aerospace Industries. This news coincided with the announcement of Indonesia's potential intention to purchase Chinese-made J-10 fighter jets and Jakarta's revision of its agreement with South Korea to procure KF-21 fighter jets. Previous Indonesian fighter jet purchases include an agreement with US manufacturer Boeing to purchase 24 F-15EX fighter jets by mid- 2023. This diversity of suppliers creates serious interoperability challenges. The use of diverse fighter jets suggests a reactive strategy designed to address pressing military needs and geopolitical pressures. The fragmented nature of these acquisitions does little to facilitate equipment operation, creates maintenance problems, reduces cross-sector training, and undermines Indonesia's long-term military strategy. For example, cross-training between Turkish, Chinese, South Korean, and American fighter jet platforms would be difficult to coordinate, effectively weakening Indonesia's regional military influence. As a result, Indonesia risks creating a fragmented military, as opposed to a coordinated modern fighting force. See Hugh Harsono, "Indonesia's Haphazard Military Acquisitions Risks Its Global Ambitions," *Small Wars Journal*, September 29, 2025, https://smallwarsjournal.com/2025/09/29/indonesia-military-acquisitions-global-ambitions/.

[316] Muhamad Haripin, Adhi Priamarizki, and Leonard C. Sebastian, "Introduction: Reform Setbacks and Selective Emulation—The Path to Military Modernization in Indonesia," in *Military Modernization and Civil-Military Relations in Indonesia*, edited by Muhamad Haripin, Adhi Priamarizki, and Leonard C. Sebastian (Singapore: Palgrave Macmillan, 2025), 1–14.

[317] Presidential Regulation of the Republic of Indonesia Number 111 of 2025 concerning General State Defense Policy for 2025-2029.

[318] Presidential Regulation of the Republic of Indonesia Number 111 of 2025 concerning General State Defense Policy for 2025-2029.

defense technology through procurement. Furthermore, a key benefit is the potential for the emergence of by-products, namely military technology reused for civilian purposes.[319] In this regard, modernization often focuses on replacing existing capabilities with superior and more lethal ones, including, among other things, the procurement of new weapons and network systems. Modernization is contextualized as part of a larger and more substantial change, namely military transformation, so it is not only associated with the hardware domain. Modernization should also extend to the software domain or the fundamental principles and doctrines that determine the procedures and guidelines for the use of military force.[320]

However, the expansion of cyber responsibility to the military significantly expands the armed forces' role within civilian governance. Military involvement in cybersecurity without a clear strategy to guide its authority is like navigating a battlefield without a compass. Military involvement in cybersecurity has the potential to trigger actions that violate civil liberties. Cybersecurity fundamentally intersects with civilian life, encompassing issues such as privacy, freedom of expression, and access to information. Giving the military a role in this area, without strict oversight and accountability, risks eroding the principles of democracy and human rights.[321]

At the same time, the Cyber Security and Resilience Bill (RUU KKS), which has been designated as a national legislative priority for 2026, still prioritizes protecting state security over protecting citizens based on human rights. This is evident in the draft RUU KKS, particularly Article 56 Paragraph (1) Letter d. The provisions in this article open up space for the involvement of the Indonesian National Armed Forces (TNI) in handling cybercrimes. According to civil society, this formulation indicates the increasingly strengthening efforts to militarize cyberspace. The draft RUU KKS also displays the character of draconian law. This is evident in the use of the term treason in cyberspace as stated in Article 61 Paragraph (2) Letter b, which carries a prison sentence of up to 20 years.[322]

A defense- and security-focused approach to regulating cyberspace has the potential to neglect the protection of citizens' fundamental freedoms and rights. Therefore, an alternative approach is needed that places rights protection as part of the cybersecurity objective. One such approach was put forward by Ronald J. Deibert, who criticized the national security-centered cybersecurity approach that prioritizes territorial sovereignty. As an alternative, he offered an approach based on human security, which places the individual as the primary object of security. In this approach, digital networks are seen as a crucial foundation for the implementation of human rights, including access to information, freedom of thought, and freedom of association. This approach also emphasizes the importance of independent oversight to ensure network security remains consistent with human rights protection. A human-centered approach should be the paradigm and logic in drafting the KKS Bill, which still strongly emphasizes national security. This approach still stems from the realist theory of world politics, where nations compete for survival and relative advantage. Therefore, the primary cybersecurity threat is understood as one that impacts sovereign states, such as damage to critical infrastructure within their jurisdiction.[323]

Meanwhile, the adoption of new military technology does not occur in a vacuum, but is influenced by domestic factors, such as political, social, economic, and cultural dynamics.

---

[319] Priamarizki and Caroline, *Prabowo's Defense Challenge*

[320] Priamarizki and Caroline, *Prabowo's Defense Challenge*

[321] Gatra Priyandita and Christian Guntur Lebang, "Indonesia's Cyber Soldiers: Armed without a Compass," *The Strategist*, April 11, 2025, https://www.aspistrategist.org.au/indonesias-cyber-soldiers-armed-without-a-compass/.

[322] Machradin Wahyudi Ritonga, "Dinilai Cederai Demokrasi, Wewenang TNI dalam RUU Keamanan dan Ketahanan Siber Jadi Sorotan," *Kompas.id*, October 4, 2025, https://www.kompas.id/artikel/dinilai-cederai-demokrasi-wewenang-tni-dalam-ruu-keamanan-dan-ketahanan-siber-jadi-sorotan.

[323] Ronald J. Deibert, "Toward a Human-Centric Approach to Cybersecurity," *Ethics & International Affairs* 32, no. 4 (2018): 411–424, https://doi.org/10.1017/S0892679418000618.

Emily O. Goldman and Andrew L. Ross emphasize situational factors and policy choices as crucial factors in determining a country's adoption path. Situational factors include geography, economic resource capacity, and the social, political, cultural, and organizational environment. Meanwhile, policy choices imply a government's commitment to a particular policy direction.[324]

In this sense, military modernization is often shaped by:[325]

1. Policy makers' perceptions of potential enemies or security threats;
2. Political and geographical understandings that influence policy makers and citizens in defining their national territory and its limitations;
3. Views and aspirations about future capabilities that must be developed to deter and defeat potential adversaries.

In addition to domestic considerations, military modernization is also influenced by the political dynamics that shape the relationship between the military and the civilian government. Thus, military modernization is determined not only by the needs and professional considerations of the military, but also by the dynamics of civil-military relations. In this context, military politicization and civilian intervention can be factors that influence, and even hinder, the military modernization process. However, military politicization can also occur due to deliberate violations by the military of civilian/non-defense matters.

Historically, the Indonesian military has been an active political actor, playing a significant role in domestic and foreign policymaking. Under the pretext of national security, for example, the military has taken the initiative to expand its role in various socio-economic (non-defense) missions and law enforcement. The military's role, particularly its authority over military operations other than war, including military modernization, will influence civil-military relations in Indonesia, particularly the recent intervention in Indonesian military politics. In this regard, there are two arguments to explain the phenomenon of civil-military relations. First, the expansion of the military's presence beyond defense is driven by the military's desire to protect its corporate interests, particularly its political supremacy. The military seeks to maintain its presence in various activities, such as civilian duties and counterterrorism. These efforts outside of defense allow for the preservation of its political influence. Second, political involvement is a product of organizational dynamics facilitated by political transactionalism with civilians.[326]

Militarization occurs not only in the realm of defense and armed conflict, but also permeates the daily lives of civilians. Paul Virilio uses the concept of pure war to describe a situation where the logic of war and military preparations persist, even in peacetime, so that the boundaries between the civilian and military spheres become increasingly blurred.[327] This idea can be linked to Stephen Graham's notion of the militarization of everyday life, which explains how military technology, practices, and logic increasingly permeate civilian life. Graham, for example, shows how militarization occurs in urban governance through the use of technologies for tracking, sorting, and profiling residents, including facial recognition software. He also highlights the tendency to view cities as threatening spaces, which contributes to the expansion of surveillance practices and the use of tactical equipment and high-powered weaponry by police. The

[324] Haripin, Priamarizki, and Sebastian, "Introduction: Reform Setbacks and Selective Emulation."
[325] Haripin, Priamarizki, and Sebastian, "Introduction: Reform Setbacks and Selective Emulation."
[326] Haripin, Priamarizki, and Sebastian, "Introduction: Reform Setbacks and Selective Emulation."
[327] After World War II, according to Paul Virilio, Western economies and societies were permanently reorganized to support military power. The focus shifted from battlefield tactics to a broader strategy, aimed at restructuring industrial society to be able to rapidly produce rockets, missiles, and other weaponry. In the context of recent advances in digital technology, computational, algorithmic, and sensing technologies have become the focal point of industrial society. See, Ben Egliston and Marcus Carter, "The Dangerous Fantasy of Cybernetic Cops," *The MIT Press Reader*, September 16, 2024, https://thereader.mitpress.mit.edu/the-dangerous-fantasy-of-cybernetic-cops/.

development of digital technology can expand these practices, particularly through increased surveillance and data collection capacity on the population.[328]

The expansion of militarization into the civilian sphere can strengthen the repressive capacity of autocratic regimes. This occurs when modern weapons technology, acquired from abroad, is increasingly used by security forces to control society. Faster and more accurate weapons allow authorities to suppress protests and unrest more effectively at lower costs. Access to modern military technology substantially reduces the likelihood of democratization in authoritarian regimes. This means that modern weapons play a key role in suppressing democratic movements. In short, more demonstrators are subjected to repressive measures by a regime with minimal resources, while simultaneously strengthening the regime.[329] The success of pro-democracy movements depends heavily on the ability or inability of the authorities to use instruments of violence against protesters, and this ability depends on weapons technology.

Because modern weapons technology has become so much more effective and cheaper, even the world's poorest countries, with the resources available to autocratic regimes today, have access to advanced weapons technology that is only a few decades old. Weapons are more cost-effective, and the technology has spread to poorer countries, giving authoritarian rulers access to powerful means of repression.[330]

Meanwhile, authoritarian governments around the world are increasingly leveraging their power to reach network operators, implement restrictive policy and legal frameworks, and acquire surveillance and censorship technologies to enhance their digital repression capabilities.[331] Asger Mose Wingender and Jacob Gerner Hariri see this phenomenon as not entirely new. Historically, the development of military technology has gone hand in hand with economic and other technological advances. In Western Europe, the need for states to finance wars led to the collection of taxes from the public. The state's dependence on these taxes, in turn, strengthened the bargaining power of citizens in demanding political rights, including the right to vote. These demands also contributed to the democratization process. However, pressure on autocratic regimes is now less intense. Weapons are now cheaper, and technology has spread to poorer countries. This situation gives authoritarian rulers access to means of repression. As a result, an imbalance has emerged between military technological development and economic growth, hindering democratization. While economic development can strengthen societal demands for democracy, at the same time, autocratic regimes' access to modern weapons technology increases the state's ability to suppress pro-democracy movements. The unbalanced development between economic modernization and advances in weapons technology can strengthen the state's position in relation to society, thus hindering the democratization process.[332]

Digital technology has given autocratic and illiberal governments unprecedented capabilities to maintain power through the use of surveillance, propaganda, and disinformation technologies. Some technologies result in far more widespread, efficient, and subtle repression and control. Digital authoritarianism takes many forms, such as online harassment, disinformation, internet blackouts, cyberattacks, and targeted surveillance using social media, artificial intelligence, and facial recognition software. Some countries, particularly the economic and technological

[328] Egliston and Carter, "The Dangerous Fantasy of Cybernetic Cops."
[329] Asger Mose Wingender and Søren Bang, "Modern Arms Technologies Help Autocratic Rulers Stay in Power," University of Copenhagen, January 25, 2023, https://news.ku.dk/all_news/2023/01/modern-arms-technologies-help-autocratic-rulers-stay-in-power.
[330] Wingender and Bang, "Modern Arms Technologies Help Autocratic Rulers Stay in Power."
[331] Irene Poetranto, "The Architecture of Digital Repression: Internet Service Providers Can Facilitate Internet Access but Also Draconian Control," Carnegie Endowment for International Peace, March 10, 2026, https://carnegieendowment.org/research/2026/03/the-architecture-of-digital-repression.
[332] Wingender and Bang, "Modern Arms Technologies Help Autocratic Rulers Stay in Power."

superpowers, are certainly more sophisticated than the tactics of leaders from developing countries. However, lower technology does not necessarily mean a lower threat. Governments with inadequate political, technological, and economic resources are still able to erode democracy and human rights.

Furthermore, it is important to understand that elements of digital authoritarianism can and do exist in liberal democracies, such as Canada and the United States. In fact, the decline of global democracy over the past 15 years has coincided with the emergence of new technologies for information gathering, communication, and surveillance. Autocratic leaders and governments have learned to harness digitalization. These leaders recognize that the survival of their regimes may depend on their ability to use digital technology as an instrument of control and repression against citizens. Authoritarianism has transformed along with the development of digital technology. This transformation is characterized by the use of digital information technology by authoritarian regimes to monitor, repress, and manipulate populations, both domestically and internationally.[333]

Authoritarian regimes, despite their sometimes democratic outward appearance, ultimately rely on repressive power and capacity. While authoritarian regimes may establish institutions that outwardly mimic a democratic framework, they are actually more interested in perpetuating their power through coercion, repression, and the suppression of dissent.[334] Repressive capacity is a key characteristic of authoritarian regimes. This capacity reflects the state's ability to use coercive power to maintain power and control society. This can be seen in the regime's ability to suppress protests and limit dissent, as well as its impact on opportunities for democratization. Repressive capacity is also related to the resources allocated to the security sector, including the budget and the number of security personnel.[335]

Tiberiu Dragu and Yonatan Lupu point out that technological developments actually strengthen the control of authoritarian regimes. Technological innovations increase the level of violations to prevent opposition groups from mobilizing and increase the likelihood that authoritarians will succeed in preventing such mobilization. This has broad implications for the human rights regime, democratization efforts, and efforts to reduce human rights violations accompanied by abuse.[336]

Furthermore, Dragu and Lupu put forward two important points in understanding the impact of digital technology on human rights under an authoritarian regime.[337] First, digital technology can strengthen preventive repression, namely the government's efforts to prevent opposition groups from mobilizing and organizing resistance. Technology allows the government to identify and monitor potential opposition groups before they become a real threat. Preventive repression can take the form of non-physical human rights violations, such as mass surveillance and censorship, but can also involve violence. In contrast to reactive repression, which is carried out in response to resistance that is already underway and can lead to mass atrocities, preventive repression aims to prevent opposition mobilization in the first place.

---

[333] Marie Lamensch, "Authoritarianism Has Been Reinvented for the Digital Age," Center for International Governance Innovation, July 9, 2021, https://www.cigionline.org/articles/authoritarianism-has-been-reinvented-for-the-digital-age/.

[334] Tiberiu Dragu and Germán Gieczewski, "Strength in Numbers? State Capacity, Military Power and Repression in Authoritarian Regimes," working paper (New York: Department of Politics, New York University; Princeton: Department of Politics, Princeton University, March 2024).

[335] However, proxy analysis for examining a regime's repressiveness may be an inaccurate indicator of repressive capacity or military strength when there is significant corruption or other agency problems within the security forces. See, Dragu and Gieczewski, "Strength in Numbers?"

[336] Dragu and Lupu, "Digital Authoritarianism and the Future of Human Rights."

[337] Dragu and Lupu, "Digital Authoritarianism and the Future of Human Rights."

Second, the impact of technology on human rights needs to be understood through the strategic interactions between authoritarian governments and opposition groups. Digital technology can enhance the capabilities of both parties, both to perpetrate repression and to mobilize resistance. However, technological innovation can also enhance the government's ability to prevent opposition mobilization while simultaneously increasing human rights violations committed in the process.

Thus, changes in digital technology have a significant impact on human rights. Digital technology empowers civil society by lowering the costs of mobilization, thus facilitating the organization of protest movements and other forms of mobilized dissent. Mobilizing public dissent is expensive, and the success of activist movements and opposition groups often depends in part on efforts to reduce these costs. Increased internet adoption correlates with transitions to democracy and higher levels of democracy, demonstrating the mobilization effect of technology in support of human rights claims.[338]

For example, in 2016, the Chinese Communist Party directed one of the largest state-owned defense contractors, China Electronics Technology Group, to develop software that could collect data on Chinese citizens' occupations, hobbies, financial transactions, and consumption habits. The request also included software to analyze citizens' online behavior and an artificial intelligence-based tool to identify faces captured on security cameras. This new surveillance system adds to the already vast data set the Chinese government has already collected. Having data on every citizen allows the government to identify those who pose a potential threat. While the stated goal of this new policy is to combat terrorism, there are concerns that its true purpose is to help silence opposition at an early stage, preventing events like Tiananmen Square and others from occurring. It is not surprising that the Chinese Communist Party is leveraging the latest developments in surveillance technology to strengthen its preventive repression efforts. In this sense, preventive repression is ex ante, carried out before protests or demonstrations occur. This differs from corrective repression, which occurs ex post, after preventive repression has failed and public protests have occurred.[339]

This situation demonstrates the paradox of new technologies that impact (1) the government's ability to preventatively silence opposition groups' efforts to mobilize public protests and (2) the ability of opposition groups to mobilize dissent. Certain technologies that can help citizens organize can also be used by authoritarian governments to silence opposition groups at an early stage; before they actually challenge the authoritarian government.[340]

No authoritarian regime wants to face a situation where dissent has grown strong enough to require large-scale military intervention to maintain power. Rulers are reluctant to make amends for military repression for at least two reasons.

First, in such an end-game scenario, the regime must rely on citizen compliance, which can be costly and ineffective. The military is untrained, ill-equipped, and unmotivated to engage in domestic repression, so using it to stifle protests is usually a last resort.

Second, asking and relying on the military involves considerable political risks in terms of regime survival, either because the military may refuse to comply with repressive orders or because the military may exploit the regime's vulnerabilities to overthrow it.[341]

---

[338] Dragu and Lupu, "Digital Authoritarianism and the Future of Human Rights."
[339] Tiberiu Dragu and Adam Przeworski, "Preventive Repression: Two Types of Moral Hazard," American Political Science Review 113, no. 1 (2019): 77–87, https://doi.org/10.1017/S0003055418000552.
[340] Dragu and Lupu, "Digital Authoritarianism and the Future of Human Rights."
[341] Dragu and Lupu, "Digital Authoritarianism and the Future of Human Rights."

William J. Dobson observes that today's authoritarian regimes have replaced brutal forms of violence and mass murder with subtle methods of control and coercion. Authoritarian regimes have perfected the use of fear and intimidation to maintain their grip on power and have learned to rely on propaganda, censorship, and co-optation as substitutes for large-scale repression against public dissent. While important, repression is only one instrument that authoritarian rulers use to maintain their power. In addition to repression, autocrats may: (1) court some potential opponents; (2) engage in propaganda; (3) engineer elections to legitimize their power or create a semblance of civil society by establishing government-operated civil society organizations. Repression is most effective when it is invisible, when the regime survives without resorting to beatings, teargassing, or killing its citizens.[342]

As a result, authoritarian regimes primarily use and rely on preventive repression, routinely carried out by specialized security agencies, typically secret police, sometimes referred to as intelligence agencies. Secret police employ professional spies and part-time informants to detect potential opposition by relying on informants, intercepting communications, planting listening devices, and the like. These measures can also include physical elimination, imprisonment, economic sanctions, travel bans, intimidation, blackmail, psychological and physical abuse, and the like. Prevention can also include censorship, the spread of false information and rumors, and the distortion of communications among opposition groups.[343]

The use of secret police (intelligence agencies) is possible because political power grants rulers, both individually and collectively, access to certain resources. To protect this power, rulers employ security agencies. In return, to carry out their duties, security agencies require the necessary resources, including buildings, vehicles, weapons, spy equipment, and funds to pay informants. Therefore, rulers must provide operational resources in addition to paying the salaries of security agents.[344]

Based on this security budget, security agencies must make decisions about the allocation of funds, determining how much will be allocated to actual protection and how much will be allocated to personal consumption. The proportion of resources agents use for personal use indicates the prevalence of corruption and other agency problems that can affect the relationship between the ruler and their security agencies. The presence of corruption suggests that not all budget resources will be allocated to actual security measures. Higher budget expenditures are at least correlated with higher repressive capacity. Conversely, when corruption levels are higher, there is a negative relationship between budget expenditures and actual repressive capacity. In cases where corruption levels are higher, this leads to increased expenditures. Paradoxically, this increase in funding is not allocated proportionally to increase actual protection.[345]

Opportunities for corruption weaken authoritarian regimes by distorting the incentives of security agencies tasked with preventing domestic opposition. Security forces can divert efforts and resources to increase their own consumption by engaging in profit-making activities that do not reduce the profits of their leaders. Secret police agents can engage in corruption, increase their expenses, sell their services to private parties, or invest in private economic ventures.[346]

In addition to the moral hazard of corruption, authoritarian regimes also face the risk of political moral hazard. This occurs when agents (security agencies) can use political influence to increase their own profits at the expense of those in power. This political risk problem is illustrated by the

[342] Dragu and Przeworski, "Preventive Repression."
[343] Dragu and Przeworski, "Preventive Repression."
[344] Dragu and Przeworski, "Preventive Repression."
[345] Dragu and Gieczewski, "Strength in Numbers?"
[346] Dragu and Przeworski, "Preventive Repression."

fact that in almost every autocratic regime, the relationship between the rulers and their security agencies is always tense. Strong security agencies are a double-edged sword for political elites. They can be more effective in protecting the regime, but they also create a moral hazard problem due to their de facto control over the instruments of violence. Security agencies can use their tools and resources to engage in political battles within the regime and to increase their political power and the associated benefits of that power over their political leaders.[347]

Reports by Tempo and several media outlets and human rights activists have found that the Indonesian government purchased large quantities of surveillance equipment from abroad between 2017 and 2023. Hundreds of these devices, worth tens of trillions of rupiah, are believed to have been secretly imported by organizations using state intermediaries. In Indonesia, these buyers include the Indonesian National Police, the State Intelligence Agency, and the National Cyber and Crypto Agency. The use of surveillance equipment is often justified by the argument that it helps law enforcement uncover crimes such as corruption and terrorism. However, without strict controls, these surveillance devices can easily be misused to monitor the movements of groups critical of the government. The clandestine purchases from countries with no diplomatic relations with Indonesia, such as Israel, indicate an attempt to evade public scrutiny and judicial control.

The clandestine purchase of surveillance equipment poses a threat to democracy and the public's right to privacy. It is also vulnerable to embezzlement and misuse. The clandestine procurement of surveillance equipment not only increases the risk of corruption but also opens the door to abuse of power. Without strong accountability systems, this technology can easily be used to spy on or suppress critical voices that are vital to the health of democracy.[348]

In addition, surveillance devices have the potential to be used by the Indonesian National Armed Forces (TNI) to support the expansion of the TNI's role in addressing cyber threats, including the TNI's involvement as a cyber security and defense investigator, which will be regulated through the Cyber Security and Resilience Law. The use of these devices indicates the Indonesian Government's tendency to use a preventive repression model to protect them from cyber threats. The Ministry of Defense once purchased sophisticated intelligence equipment from the UK for £4.21 million or the equivalent of Rp71.35 billion, called Finfisher. This device is effective for tapping into a person's activities via the internet and mobile phones. According to the United Kingdom (UK) Export Finance report document for the 2012-2013 period, there was a transaction for the sale and purchase of intelligence equipment between the Indonesian government represented by Defense Minister Purnomo Yusgiantoro and Gamma TSE Ltd. Indeed, the document does not detail what tools were included in the transaction.[349] FinFisher's FinSpy spyware has previously been linked to Indonesia. In March 2013, Citizen Lab published a report based on internet scanning measurements that identified FinSpy customer servers hosted in Indonesia. A follow-up publication in 2015 based on Citizen Lab's internet scanning linked FinFisher servers to the National Crypto Agency (Badan Ciber dan Cipher) which in 2017 changed its name to the National Cyber and Crypto Agency.[350]

Social media surveillance efforts can also be traced during the COVID-19 pandemic. The Indonesian National Police Headquarters (Mabes Polri) has officially issued a telegram containing guidelines for law enforcement in handling criminal acts amidst the coronavirus (COVID-19) outbreak. The National Police has increased social media monitoring as an effort to

[347] Dragu and Przeworski, "Preventive Repression."
[348] Tempo Editorial, "The Dark Threat of Surveillance Equipment," *Tempo.co*, May 9 2024, https://en.tempo.co/read/1865183/the-dark-threat-of-surveillance-equipment.
[349] Kontan.co.id, "Kemhan Beli Penyadap Canggih Rp 71,35 Miliar," https://nasional.kontan.co.id/news/kemhan-beli-penyadap-canggih-rp-7135-miliar.
[350] Amnesty International, *A Web of Surveillance*.

prevent the spread of false information and comments that defame the President and government officials during the COVID-19 outbreak.[351] Then a social media monitoring system procurement package worth IDR 49.2 billion by the Ministry of Defense in the 2026 budget year through direct appointment with the Indonesian Army Headquarters work unit (satker), shows this trend.[352]

The increasing use of commercial spyware and other types of surveillance technology by governments poses a serious threat to human rights worldwide. Police and intelligence services in many countries use such technology to target activists, journalists, humanitarians, academics, and other critical voices, undermining democratic institutions, narrowing civic space, violating the privacy and other rights of victims, and in many cases, threatening their physical security.[353] Spyware threatens the privacy rights of targeted individuals. While certain intrusions on privacy are permissible, international human rights law stipulates that any restriction of legitimate rights must be provided by law, pursue a legitimate aim, and be proportionate, meaning no more than is necessary in a democratic society.[354] When spyware technology is used within the boundaries of a legitimate aim, proportionality remains debatable, given its intrusive nature, as spyware infections can provide access and expose, among other things, communications, geolocation, camera, and microphone data on targeted devices. This allows not only real-time but also retrospective access to data on targeted individuals and others they interact with, turning mobile phones into what the Office of the United Nations High Commissioner for Human Rights (OHCHR) calls 24/7 surveillance devices. For many targets of spyware, the violation of their fundamental right to privacy is obvious. This can mean the intrusion is so severe that the individual forfeits that right.

In May 2019, David Kaye, the UN Special Rapporteur on freedom of opinion and expression, expressed serious concerns about the status of surveillance exports. In the report, the UN Special Rapporteur explained that digital surveillance is no longer the prerogative of countries with the internal resources to conduct mass and targeted surveillance. The Special Rapporteur emphasized that countries purchasing surveillance technology must take steps to ensure that its use is consistent with international human rights law, including strengthening national laws to limit surveillance, creating public mechanisms for the approval and oversight of surveillance technologies, and ensuring that victims of violations have domestic legal means to seek redress.[355]

The Special Rapporteur further stated:[356]

> "Surveillance targets experience an intrusion into their privacy rights and freedom of opinion and expression, whether the surveillance attempt is successful or not. The target

[351] The official telegram was signed by the Head of the Criminal Investigation Agency (Kabareskrim), Commissioner General Listyo Sigit Prabowo, on April 4, 2020. The three main types of violations that will be monitored by the police cyber patrol include the spread of hoaxes related to the coronavirus, statements that corner the government and the President, and online fraud related to the sale of health equipment. See, Dimas Kuncoro, "Coronavirus Crackdown Aimed at Anti-President Smears, Hoaxes," *Tempo.co*, April 6, 2020, https://en.tempo.co/read/1328272/coronavirus-crackdown-aimed-at-anti-president-smears-hoaxes.

[352] Kompas.id, "Anggaran Rp 492 Miliar untuk Monitoring Medsos TNI AD Dipertanyakan Publik," April 28, 2026, https://www.kompas.id/artikel/anggaran-rp-492-miliar-untuk-monitoring-medsos-tni-ad-dipertanyakan-publik.

[353] Human Rights Watch, *Looking the Other Way: EU Failure to Prevent Surveillance Exports to Rights Violators* (12 May 2026), https://www.hrw.org/report/2026/05/12/looking-the-other-way/eu-failure-to-prevent-surveillance-exports-to-rights.

[354] Riecke, "Unmasking the Term 'Dual Use' in EU Spyware Export Control."

[355] David Kaye, *Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, A/HRC/41/35 (Geneva: United Nations, 28 May 2019), https://digitallibrary.un.org/record/3814512.

[356] Kaye, *Surveillance and Human Rights*.

does not need to be aware of the attempted or successful intrusion for the intrusion to be complete."

Such disruption is part of an overall effort to inflict consequences on the target. If carried out for unlawful purposes, successful surveillance and operations can be used to silence dissent and sanction criticism.

In an atmosphere of illegal surveillance, it will shape and limit their ability to exercise their rights to freedom of expression, association, religious belief, culture, and so on."[357]

The report of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age reinforces the Special Rapporteur's view:[358]

> "State actors often appear to pursue objectives that are illegitimate under international human rights law. While, in certain circumstances, surveillance measures may be permissible under articles 17 and 19 of the International Covenant on Civil and Political Rights for the protection of national security or public order, hacking can never be justified for political or business reasons, which is often the case when human rights defenders or journalists are targeted.
>
> Even when legitimate objectives are being pursued, such as national security or the protection of others' rights, judgments about the necessity and proportionality of the use of spyware severely limit the permissible uses of spyware. There is a strong argument that tools like Pegasus, which allow unrestricted intrusion into individuals' lives and access to their inner thoughts, thus affect the very essence of the right to privacy and impinge on the absolute right to freedom of thought and expression."

A similar view was expressed by Fionnuala Ní Aoláin, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism:[359]

> "The scale of human rights violations caused by the proliferation and misuse of sophisticated and invasive cybersurveillance technologies worldwide, initially justified or intended for counter-terrorism and national security purposes. Advanced surveillance technologies developed for counter-terrorism and national security purposes have increasingly come under international scrutiny due to a series of revelations showing that these tools are actually being used to spy on politicians, journalists, human rights activists, advocates, and ordinary citizens who have no links to terrorism and pose no national security threat. Intrusive covert technologies for surveillance of the content of individuals' digital communications and other information, including metadata (location, duration, source, and contacts), commonly known as spyware, have proliferated internationally, spiraling out of control and posing significant risks to the promotion and protection of human rights.

---

[357] The Special Rapporteur referred to the International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights, which protect everyone's right to privacy, opinion and expression. Article 19 of both instruments protects everyone's right to hold opinions without interference and to seek, receive and impart information and ideas of all kinds, regardless of frontiers and through any media. Article 17(1) of the Covenant, echoing article 12 of the Declaration, states that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence. See Kaye, *Surveillance and Human Rights*.

[358] Office of the United Nations High Commissioner for Human Rights (OHCHR), *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights*, A/HRC/51/17 (Geneva: United Nations, 4 August 2022), https://digitallibrary.un.org/record/3985679.

[359] Fionnuala Ní Aoláin, *Human Rights Implications of the Development, Use and Transfer of New Technologies in the Context of Counter-Terrorism and Countering and Preventing Violent Extremism: Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, A/HRC/52/39 (Geneva: United Nations, 1 March 2023), https://digitallibrary.un.org/record/4031525.

> The impact of surveillance on various human rights is profound, and the Special Rapporteur emphasizes that the right to privacy serves as a fundamental right that protects and enables many other rights and freedoms, and its protection is closely linked to the existence and progress of democratic societies. Therefore, the increasing use of covert surveillance and the collection of content and metadata information for the purpose of combating terrorism, combined with the rapid development of new, poorly regulated technologies, constitutes a significant threat to democratic societies."

Fionnuala Ní Aoláin further identified serious violations of international human rights law in the various consequences of the use of surveillance tools, particularly spyware. These violations include: (1) violations of the right to life; (2) exposure to unlawful physical violence (including sexual violence), unlawful arrest, and/or harassment from government or private actors; (3) disproportionate interference with individuals' right to privacy; (4) disproportionate interference with the rights to freedom of expression, freedom of association, and freedom of religion; (5) the production and reinforcement of gender-specific harms including direct harms to women and girls, and sexual minorities (LGBTQI+); (6) interference with the integrity of records and documentary evidence, which undermines procedural fairness and the rule of law; and (7) obstacles to individuals' ability to obtain redress and effective remedies for violations of their human rights.[360]

A similar view was expressed by Gina Romero, acting in her capacity as Special Rapporteur:[361]

> Invasive, pervasive, and high-risk digital systems, often inherently incompatible with human rights obligations, are often inappropriately justified through narratives of security and crime prevention. This often involves sweeping claims about national security, sovereignty, terrorism, public safety, transnational crime, cybersecurity, hate crimes, "moral crimes," disinformation, and the like. Civil and political activism are increasingly used as opportunities for surveillance.
>
> Associations and groups are frequently labeled as "national security threats," "foreign agents," "criminals," or "terrorists." Authorities employ a mix of covert, stealthy, and online surveillance strategies, including data harvesting, alongside more overt and visible forms, such as surveillance drones. This normalizes the development of invasive surveillance infrastructure, even in democracies.
>
> Countries have adopted overly broad measures that expand surveillance while neglecting transparency, public oversight, and human rights protection. This shift to a preventive paradigm fundamentally erodes the presumption of innocence and due process by forcing individuals to prove they pose no threat. At the same time, the State effectively reverses the burden of proof, facilitating the widespread criminalization of activists, transforming the digital environment into a space of permanent suspicion.

The European Court of Human Rights has elaborated on this proportionality test by providing minimum safeguards "which must be established by law to avoid abuse of power" during targeted surveillance operations. In principle, the use of spyware for law enforcement and counter-terrorism purposes can pursue legitimate objectives, such as the protection of national security or public order. From the perspective of the European Data Protection Supervisor, this

---

[360] Fionnuala Ní Aoláin, *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach, position paper* (Geneva: Office of the United Nations High Commissioner for Human Rights, April 2023), https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf

[361] Gina Romero, *Unmasking the Chilling Effects of the Digital Surveillance Ecosystem: The Erosion of Assembly and Association Rights: Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association*, A/HRC/62/45(Geneva:UnitedNations,21April2026), https://digitallibrary.un.org/record/4113878.

would only apply to situations of extremely serious threat, such as an imminent terrorist attack. Furthermore, the EDPS cautions that such cases are exceptional and cannot justify a more widespread or systematic deployment of highly invasive technology.[362]

Since the use of spyware has implications for the right to life, Fionnuala Ní Aoláin refers to the UN Human Rights Committee[363] in its General Comment 36 on the Right to Life, 2019, to articulate corporate responsibility:[364]

> "States must exercise due diligence to protect the lives of individuals from deprivation caused by persons or entities whose conduct is not attributable to the State. This involves taking special protective measures for people in vulnerable situations whose lives have been placed at particular risk due to specific threats or pre-existing patterns of violence, including human rights defenders, officials fighting corruption and organized crime, humanitarian workers, journalists, prominent public figures, witnesses to crimes and victims of domestic and gender-based violence and human trafficking."

The State's obligation to respect and protect human life goes even further, as stated in General Comment 36:[365]

1. States Parties shall take appropriate measures to protect individuals from deprivation of life by other States, international organizations and foreign companies operating in their territory or in other areas under their jurisdiction;
2. States shall also take appropriate legislative and other measures to ensure that all activities occurring wholly or partly in their territory and in other places under their jurisdiction, but having a direct and reasonably foreseeable impact on the right to life of individuals outside their territory, including activities carried out by enterprises based in their territory or under their jurisdiction, are in accordance with Article 6 of the Covenant on Civil and Political Rights, taking into account international standards relating to corporate responsibility, and the right of victims to an effective remedy.

Gina Romero reiterates the importance of business responsibility in strengthening human rights protections for those affected by the use of surveillance technology:[366]

> "This is coupled with a lack of political will to regulate high-risk surveillance technologies, some of which may be inherently incompatible with states' human rights obligations. This is often driven by opaque state-corporate collaborations that disregard human rights obligations, and coercive pressure from states and corporations to remove safeguards that prevent misuse or inappropriate use."

David Kaye, recommended an immediate moratorium on the sale and transfer of such technology until international regulations with human rights protections were implemented.[367] This recommendation was later reaffirmed by UN human rights experts[368] who call on all States

---

[362] Riecke, "Unmasking the Term 'Dual Use' in EU Spyware Export Control."

[363] A specialized body of experts tasked with providing authoritative guidance on the interpretation of human rights standards set out in the International Covenant on Civil and Political Rights

[364] Fionnuala Ní Aoláin and Adriana Edmeades Jones, "Spyware Out of the Shadows: The Need for a New International Regulatory Approach,"Just Security, May 16, 2023, https://www.justsecurity.org/86558/spyware-out-of-the-shadows-the-need-for-a-new-international-regulatory-approach/.

[365] Ní Aoláin and Edmeades Jones, "Spyware Out of the Shadows."

[366] Romero, *Unmasking the Chilling Effects of the Digital Surveillance Ecosystem*.

[367] Kaye, *Surveillance and Human Rights*.

[368] The experts are Irene Khan, Special Rapporteur on the promotion and protection of the right to freedom of expression; Mary Lawlor, Special Rapporteur on the situation of human rights defenders; Clement Nyaletsossi Voulé, Special Rapporteur on the right to freedom of peaceful assembly and of association; and the UN Working Group on human rights and transnational corporations and other business enterprises (known as the Working Group on Business and Human Rights), consisting of Surya Deva (Chair), Elzbieta Karska (Vice-Chair), Githu Muigai, Dante

to impose a global moratorium on the sale and transfer of surveillance technology until they implement strong regulations that ensure its use is in accordance with international human rights standards:[369]

> "It is extremely dangerous and irresponsible to allow the surveillance technology and trade sectors to operate as human rights-free zones.
>
> Highly sophisticated and intrusive tools are being used to monitor, intimidate, and silence human rights defenders, journalists, and political opponents. These practices violate the rights to freedom of expression, privacy, and liberty, potentially endangering the lives of hundreds of individuals, jeopardizing media freedom, and undermining democracy, peace, security, and international cooperation.
>
> Given the extraordinary affront to human rights demonstrated by its extensive use of surveillance, NSO Group should disclose whether it has ever conducted meaningful human rights due diligence in accordance with the UN Guiding Principles on Business and Human Rights and fully publish the findings of any internal investigations it may have conducted into this matter.
>
> Urges Israel, as the country of origin of NSO Group, to fully disclose the steps it has taken to review NSO's export transactions in light of Israel's inherent human rights obligations. It is the state's obligation to verify that companies like NSO Group do not sell or transfer technology to or contract with countries and entities that are likely to use it to violate human rights.

Amnesty International also recommends the importance of enforcing regulations on dual-use technologies to address the proliferation of highly invasive spyware and other surveillance technologies, which pose a serious threat to human rights. Such highly invasive spyware tools can be used covertly to conduct highly intrusive surveillance of civil society and suppress freedom of expression, which can have chilling effects. Without effective enforcement mechanisms, these technologies can be easily exported and exploited, leading to egregious human rights violations and abuses, including the right to privacy. The development of dual-use technologies relies on components and infrastructure that may not be subject to dual-use regulations but are an integral part of the system's function with potential military applications.

Furthermore, the reliance on countries that export non-dual-use technologies essential to the operation of dual-use systems further underscores the importance of law enforcement efforts in upholding human rights. By ensuring strict enforcement of regulations governing the export and transfer of non-dual-use goods, governments can prevent the proliferation of dual-use systems that threaten human rights. Collaborative efforts between exporting and importing countries are essential to establish comprehensive controls that cover the entire spectrum of technologies involved in dual-use systems, thereby promoting accountability and protecting against misuse.[370]

Pesce, and Anita Ramasastry. See, Office of the United Nations High Commissioner for Human Rights (OHCHR), "Spyware Scandal: UN Experts Call for Moratorium on Sale of 'Life Threatening' Surveillance Tech," August 12, 2021, https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening?LangID=E&NewsID=27379.

[369] OHCHR, "Spyware Scandal: UN Experts Call for Moratorium on Sale of 'Life Threatening' Surveillance Tech."

[370] Amnesty International, *A Web of Surveillance*.

CHAPTER III
CONCLUSION AND RECOMMENDATIONS

Conclusion

The militarization of technology is a far broader process than simply the use of technology by military institutions. The development of artificial intelligence, drones, surveillance technology, spyware, and so on has transformed the character of contemporary defense and security. Technologies previously developed for civilian and commercial purposes can be rapidly adapted for intelligence, surveillance, target identification, decision-making, and even the use of force. This dual-use nature makes the separation between civilian and military spheres increasingly difficult to maintain.

These changes are occurring concurrently with the transformation of the military-industrial complex into an increasingly digital ecosystem. While the classic military-industrial complex describes the relationship between governments, military institutions, and the arms industry, current developments are expanding this network with the entry of technology companies, cloud providers, AI companies, chip manufacturers, telecommunications companies, defense tech startups, and even surveillance technology providers. Thus, military capacity worldwide is now built not only through the ownership of tanks, fighter jets, or weapons but also through the control of data, algorithms, sensors, communications infrastructure, and computing capabilities. In this relationship, security needs generate budgets and procurement that create markets for industry, while economic interests and industrial technological capacity can again influence how threats and defense needs are defined.

In the Indonesian context, these symptoms are evident through the modernization of weapons systems, increased defense spending, strengthening of the national defense industry, and increasing attention to AI, unmanned systems, surveillance, and cyber defense. This research found that the technological militarization ecosystem is formed through four elements: (1) technology, (2) state institutions (3), the military, and (4) the defense industry and the private sector/big tech companies. The role of the military is also increasingly intersecting with non-military domains, including cyberspace, as stipulated in Law No. 3 of 2025 concerning Amendments to Law No. 34 of 2004 concerning the Indonesian National Armed Forces (TNI), and increased authority in Article 7 Paragraph (2) letter b number 15 Military Operations Other Than War (MOOTW) regarding Cyber Defense Threats.

The human rights issue is becoming increasingly important because digital technology fundamentally enhances the state's capacity to see, know, identify, connect, classify, and take action against individuals. However, this growing capacity has not been fully matched by a comparable regulatory and oversight system. The challenge lies not in how far states can adopt new technologies, but rather in ensuring that this increased capacity does not result in increased power without increased accountability.

Recommendations

This research recommends several things that can be implemented at the national level. These recommendations are as follows:

1. Strengthen substantive civilian oversight of the procurement and use of defense technology, including through the House of Representatives (DPR), the National Commission on Human Rights (Komnas HAM), and the Indonesian Ombudsman (ORI).

2. Establish a clear legal basis for the use of high-risk technologies such as spyware, AI surveillance, biometrics, and autonomous systems.
3. Promote accountability of Big Technology Companies and private companies through human rights due diligence, audits, and clarity of jurisdiction and legal responsibility.
4. Ensure effective complaint and redress mechanisms for victims of technology abuse, including illegal surveillance and AI-based violations.

Bibliography

Akbar, Adrial. “Rapat Tertutup di DPR, Menhan-Panglima TNI Usul Tambah Anggaran Rp 184 T.” detikNews, July 9, 2025. https://news.detik.com/berita/d-8003834/rapat-tertutup-di-dpr-menhan-panglima-tni-usul-tambah-anggaran-rp-184-t.

Al Jazeera. “Egypt Blocks Human Rights Watch Website.” September 8, 2017. https://www.aljazeera.com/news/2017/9/8/egypt-blocks-human-rights-watch-website.

———. “Israel Retrofitting DJI Commercial Drones to Bomb and Surveil Gaza.” 8 May 2025. https://www.aljazeera.com/news/2025/5/8/israel-retrofitting-dji-commercial-drones-to-bomb-and-surveill-gaza.

Albanese, Francesca. *From Economy of Occupation to Economy of Genocide*. Report of the Special Rapporteur on the Situation of Human Rights in the Palestinian Territories Occupied since 1967. UNDoc.A/HRC/59/23. UnitedNations, June 30, 2025. https://www.ohchr.org/en/documents/country-reports/ahrc5923-report-special-rapporteur-situation-human-rights-palestinian.

———. *Report of the Special Rapporteur on the Situation of Human Rights in the Palestinian Territories Occupied since 1967: Gaza Genocide: A Collective Crime*. A/80/492. New York: United Nations, 20 October 2025.

Amnesty International. *A Web of Surveillance: Unraveling a Murky Network of Spyware Exports to Indonesia*. ASA21/7974/2024. May 1, 2024. https://www.amnesty.org/en/documents/asa21/7974/2024/en/.

———. “Indonesia: Military Silences Dissent with Disinformation Campaigns Branding Activists and Journalists ’Foreign Agents’.” May 10, 2026. https://www.amnesty.org/en/latest/news/2026/05/indonesia-military-silences-dissent-disinformation-campaigns-branding-activists-journalists-foreign-agents/.

———. *Membangun Musuh Khayalan: Misinformasi, Disinformasi dan Tuduhan “Antek Asing” di Bawah Presiden Prabowo di Indonesia*. ASA 21/0931/2026. May 19, 2026. https://www.amnesty.org/en/documents/asa21/0931/2026/id/.

Amnesty International Indonesia “‘Arus Balik’ Hak Asasi Manusia di 100 Hari Pemerintahan Baru.” January 21, 2025. https://www.amnesty.id/kabar-terbaru/siaran-pers/arus-balik-hak-asasi-manusia-di-100-hari-pemerintahan-baru/01/2025/.

Amnesty International Security Lab and Citizen Lab. “Devices of Palestinian Human Rights Defenders Hacked with NSO Group’s Pegasus Spyware.” 8 November 2021. https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/.

Angendari, Dewa Ayu Diah. “Militerisme di Media Sosial: Bagaimana UU TNI Mengancam Kebebasan Sipil di Dunia Siber,” *The Conversation*. https://theconversation.com/militerisme-di-media-sosial-bagaimana-uu-tni-mengancam-kebebasan-sipil-di-dunia-siber-254065.

Arifianto, Y. *Sistem Pengelolaan Anggaran Belanja Militer di Indonesia: Tinjauan Aspek Pengendalian, Transparansi dan Akuntabilitas Publik*. Master’s thesis, University of Indonesia, 2005. https://lib.ui.ac.id/detail?id=83595&lokasi=lokal.

ASEAN Parliamentarians for Human Rights (APHR). “Indonesia Must Halt the Import and Use of Highly Invasive Spyware from Israel and Elsewhere, Southeast Asian MPs Say.” May 6, 2024. https://aseanmp.org/publications/post/indonesia-must-halt-the-import-and-use-of-highly-invasive-spyware-from-israel-and-elsewhere-southeast-asian-mps-say/.

Defense Technology Agency, Ministry of Defense of the Republic of Indonesia. “Design Requirement Rancang Bangun Weapon Integration System PTTA MALE Konsorsium.” July 7, 2025. https://www.kemhan.go.id/batekhan/2025/07/07/design-requirement-rancang-bangun-weapon-integration-system-ptta-male-konsorsium.html.

Basu, Arindrajit, and Gatra Priyandita. “Why Haven’t India and Indonesia Signed Up for Anti-Spyware Dialogue?” *Royal United Services Institute*, April 10, 2024. https://www.rusi.org/explore-our-research/publications/commentary/why-havent-india-and-indonesia-signed-anti-spyware-dialogue.

BBC News Indonesia. “Aparat membungkam jurnalis dan aktivis dengan narasi antek asing, sebut laporan.” May 20, 2026. https://www.bbc.com/indonesia/articles/cj4pqkw785lo.

Bego, Katja. “How a Surge in Defense and Dual-Use Technology Investment Could Reconfigure the Global AI Race.” *Chatham House*, April 28, 2026. https://www.chathamhouse.org/2026/04/how-surge-defence-and-dual-use-technology-investment-could-reconfigure-global-ai-race/02.

Breger, Michael. “The Legacies of Militarization: Norman Joshua Writes a Social and Cultural History of Indonesian Authoritarianism.” FSI, Stanford University, 17 April 2024. https://fsi.stanford.edu/news/legacies-militarization-norman-joshua-writes-social-cultural-history-indonesian.

Business & Human Rights Resource Center. “Palantir & Starlink Allegedly Complicit in War Crimes amid Israel’s War on Gaza.” June 6, 2024. https://www.business-humanrights.org/en/latest-news/palantir-spacex-allegedly-complicit-in-war-crimes-amid-israels-war-in-gaza/.

Castells, Manuel. The Rise of the Network Society. 2nd ed. Chichester: Wiley-Blackwell, 2010.

Central Intelligence Agency (CIA). “The Enigma of Alan Turing.” April 10, 2015. https://www.cia.gov/stories/story/the-enigma-of-alan-turing/.

Chin Human Rights Organization (CHRO) and Myanmar Accountability Project (MAP). “Indonesian Arms Producers Accused of Illegal Sales to Myanmar.” October 2, 2023. https://progressivevoicemyanmar.org/2023/10/02/press-release-indonesian-arms-producers-accused-of-illegal-sales-to-myanmar.

CNN Indonesia. “Pemerintah Siapkan Rp329,5 Triliun untuk Pertahanan di RAPBN 2027.” August 19, 2026. https://www.cnnindonesia.com/nasional/20260819113956-20-1393907/pemerintah-siapkan-rp3295-triliun-untuk-pertahanan-di-rapbn-2027.

Corporate Watch. “What’s Driving the Militarization of Tech—and What We Can Do about It.” https://corporatewatch.org/whats-driving-the-militarisation-of-tech-and-what-we-can-do-about-it/.

Coveri, Andrea, Claudio Cozza, and Dario Guarascio. “Big Tech and the US Digital-Military-Industrial Complex.” Intereconomics 60, no. 2 (2025): 81–87. https://doi.org/10.2478/ie-2025-0017.

Cronin-Furman, Kate. *Hypocrisy and Human Rights: Resisting Accountability for Mass Atrocities*. Ithaca, NY: Cornell University Press, 2022.

Damrosch, Lori F. “Gross and Systematic Human Rights Violations.” *Max Planck Encyclopedia of Public International Law*. Oxford University Press,2011. https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1732.

de Búrca, Gráinne, and Katharine G. Young. “The (Mis)appropriation of Human Rights by the New Global Right: An Introduction to the Symposium.” *International Journal of Constitutional Law* 21, no. 1 (January 2023).

Deibert, Ronald J. “Toward a Human-Centric Approach to Cybersecurity.” *Ethics & International Affairs* 32, no. 4 (2018): 411–424. https://doi.org/10.1017/S0892679418000618.

Deikin, Alexander. *An Alliance of the Monopolies and the Military: On the US Military-Industrial Complex*. Moscow: Novosti Press Agency, 1973.

delle Fave, Danilo. “The Challenges of Dual-Use Space Technologies: The Non-Peaceful Use of Satellites.” *Space Generation Advisory Council*, April 14, 2023. https://spacegeneration.org/the-challenges-of-dual-use-space-technologies-the-non-peaceful-use-of-satellites.

Defense Advanced Research Projects Agency (DARPA).” AI Next.” https://www.darpa.mil/research/programs/ai-next.

———. “Breakthrough Technologies for National Security.” 2015.

Detik.com. “Rapat Komisi I DPR, Panglima TNI Tertutup Saat Bahas Alutsista.” October 22, 2024. https://news.detik.com/berita/d-5560339/rapat-komisi-i-dpr-panglima-tni-tertutup-saat-bahas-alutsista.

Deutsche Welle. “Points from Prabowoso’s Statement on Palestine at the KTTPBB.” https://www.dw.com/id/poin-poin-pernyataan-prabowo-soal-palestina-di-ktt-pbb/a-74102466.

Dragu, Tiberiu, and Germán Gieczewski. “Strength in Numbers? State Capacity, Military Power and Repression in Authoritarian Regimes.” Working papers. New York: Department of Politics, New York University; Princeton: Department of Politics, Princeton University, March 2024.

Dwipratama, Gede Priana. “Swarm Drones: Tantangan, Peluang dan Ancaman bagi Indonesia.” Directorate General of Defense Potential, Ministry of Defense of the Republic of Indonesia, April 25, 2024. https://www.kemhan.go.id/pothan/2024/04/25/swarm-drone-tantangan-peluang-dan-ancaman-bagi-indonesia.html.

Egliston, Ben, and Marcus Carter. “The Dangerous Fantasy of Cybernetic Cops.” The MIT Press Reader, September 16, 2024. https://thereader.mitpress.mit.edu/the-dangerous-fantasy-of-cybernetic-cops/.

Eide, Asbjorn. *The Universal Declaration of Human Rights: A Commentary*. Oslo: Scandinavian University Press, 1992.

Elistair. “Intelligence, Surveillance, and Reconnaissance (ISR).” https://elistair.com/glossary/intelligence-surveillance-reconnaissance/.

ELSAM. “Peneliti ELSAM Peringatkan Potensi Militerisasi Ruang Digital lewat RUU Keamanan dan Ketahanan Siber (RUU KKS).” October 21, 2025. https://www.elsam.or.id/teknologi-dan-ham/peneliti-elsam-peringatkan-potensi-militerisasi-ruang-digital-lewat-ruu-keamanan-dan-ketahanan-siber%E2%80%93ruu-kks-.

———. “UU Perlindungan Data Pribadi Mendesak untuk Menjamin Kedaulatan Individu di Ruang Siber.” 2025. https://www.elsam.or.id/siaran-pers/uu-perlindungan-data-pribadi-mendesak-untuk-menjamin-kedaulatan-individu-di-ruang-siber.

Evron, Yoram, and Richard A. Bitzinger. *The Fourth Industrial Revolution and Military-Civil Fusion: A New Paradigm for Military Innovation?* Cambridge: Cambridge University Press, 2023.

Faridi, Rushad. “Starlink in Gaza: Humanitarian Lifeline or Military Asset?” *The Daily Star*, September 9, 2025. https://www.thedailystar.net/slow-reads/focus/news/starlink-gaza-humanitarian-lifeline-or-military-asset-3981756.

Fatafta, Marwa. “Egypt’s New Data Protection Law: Data Protection or Data Control?” *Access Now*, September 24, 2020. https://www.accessnow.org/egypts-new-data-protection-law-data-protection-or-data-control/.

Fauzi, Elfian, and Nabila Alif Radika Shandy. “Hak Atas Privasi dan Politik Hukum UndangUndang Nomor 27 Tahun 2022 tentang Pelindungan Data.” *LEX Renaissance* 7, no. 3 (July 7, 2022): 445–461.

Foreign & Commonwealth Office and Foreign, Commonwealth & Development Office. “The UK and International Humanitarian Law.” GOV.UK. July 24, 2018, updated April 4, 2024. https://www.gov.uk/government/publications/international-humanitarian-law-and-the-uk-government/uk-and-international-humanitarian-law-2018.

Freedom House. “Egypt.” *Freedom on the Net 2022*. 2022. https://freedomhouse.org/country/egypt/freedom-net/2022.

Frenkel, Sheera. “The Militarization of Silicon Valley.” *The New York Times*, August 4, 2025. https://www.nytimes.com/2025/08/04/technology/google-meta-openai-military-war.html.

Godsin, Manuel. “Rheinmetall Denel Faces Scrutiny over Allegations of Arms Use in Sudan Conflict.” *Sunday Independent / The Star*, July 8, 2025. https://thestar.co.za/sundayindependent/news/2025-07-08-rheinmetall-denel-faces-scrutiny-over-allegations-of-arms-use-in-sudan-conflict/.

González, Roberto J. How Big Tech and Silicon Valley Are Transforming the Military-Industrial Complex. Costs of War, Watson Institute for International and Public Affairs, Brown University, April 17, 2024. https://costsofwar.watson.brown.edu/paper/how-big-tech-and-silicon-valley-are-transforming-military-industrial-complex.

Goodman, Matthew P., Matthew Reynolds, and Julianne Fittipaldi. *Economic Security in Emerging Markets: A Look at India, Vietnam, and Indonesia*. CSIS Briefs. Washington, DC: Center for Strategic and International Studies (CSIS), May 17, 2022. https://www.csis.org/analysis/economic-security-emerging-markets-look-india-vietnam-and-indonesia.

Gorbanova, Mariya, and Leah Wawro. *The Transparency of National Defense Budgets: An Initial Review*. London: Transparency International UK, 2011.

Hafiez, Fachri Audhia. “Rapat Bahas Anggaran Alutsista Menhan dengan Komisi I DPR Digelar Tertutup.” MetroTVNews.com, June 12, 2024. https://www.metrotvnews.com/read/bD2C1Qj6-rapat-bahas-anggaran-alutsista-menhan-dengan-komisi-i-dpr-digelar-tertutup.

Haripin, Muhammad. *Civil-Military Relations in Indonesia: The Politics of Military Operations Other Than War*. Abingdon: Routledge, 2020.

———.”Indonesian Parliament Passes Law Expanding Military’s Role in Government.” ADRN Issue Briefing, 17 April 2025. http://adrnresearch.org/publications/list.php?cid=2&idx=407&ckattempt=3.

Haripin, Muhamad, Adhi Priamarizki, and Leonard C. Sebastian. “Introduction: Reform Setbacks and Selective Emulation—The Path to Military Modernization in Indonesia.” In *Military Modernization and Civil-Military Relations in Indonesia*, edited by Muhamad Haripin, Adhi Priamarizki, and Leonard C. Sebastian, 1–14. Singapore: Palgrave Macmillan, 2025.

Haripin, Muhamad, and Adhi Priamarizki. “Jokowi Consolidates Influence over TNI as Elections Loom.” *New Mandala*. https://www.newmandala.org/jokowi-consolidates-influence-over-tni-as-elections-loom/.

Harsono, Hugh. “Indonesia’s Hazardous Military Acquisitions Risk Its Global Ambitions.” *Small Wars Journal*, September 29, 2025. https://smallwarsjournal.com/2025/09/29/indonesia-military-acquisitions-global-ambitions/.

Harun, Umar. *Perkembangan Politik Internasional Era Perang Dingin dan Globalisasi*. Jakarta: National University Publishing Institute, 2022.

Hasiana, Dovana. “Anggaran Pertahanan 2025 Dipatok Naik 47% Jadi Rp245 Triliun.” *Bloomberg Technoz*, July 6, 2025. https://www.bloombergtechnoz.com/detail-news/76302/anggaran-pertahanan-2025-dipatok-naik-47-jadi-rp245-triliun.

Henschke, Adam. *Ethics in an Age of Surveillance: Personal Information and Virtual Identities*. Cambridge: Cambridge University Press, 2017.

Hinton, James W. *Dual-Use Technologies in the Age of Intangibles*. Policy Brief No. 215. Waterloo, ON: Center for International Governance Innovation (CIGI), November 3, 2025. https://www.cigionline.org/publications/dual-use-technologies-in-the-age-of-intangibles/.

Human Rights Watch. *Looking the Other Way: EU Failure to Prevent Surveillance Exports to Rights Violators*. May 12, 2026. https://www.hrw.org/report/2026/05/12/looking-the-other-way/eu-failure-to-prevent-surveillance-exports-to-rights.

———. “Myanmar: Facial Recognition System Threatens Rights: Camera Surveillance, Mass Data Collection Bolsters Abusive Junta.” March 12, 2021. https://www.hrw.org/news/2021/03/12/myanmar-facial-recognition-system-threatens-rights.

Ikrom, Moh Bagas Fadhli Dzil, and Badrut Tamam. “Perlindungan Hukum Hak Privasi Warga Negara terhadap Kebocoran Data Pribadi di Indonesia.” *Jurnal Konstitusi* 3, no. 2 (December 2024).

Indonesia Defense. “Spesifikasi Drone Baru untuk Tugas Operasi Prajurit Marinir di Perbatasan.” April 17, 2024. https://indonesiadefense.com/spesfiikasi-drone-baru-untuk-tugas-operasi-prajurit-marinir-di-perbatasan/.

International Committee of the Red Cross. “Methods and Means of Warfare.”

———. *Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach*. June 2019.

Jili, B. “The Rise of Chinese Surveillance Technology in Africa.” *Electronic Privacy Information Center (EPIC)*, May 31, 2022. https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa/.

Ministry of Foreign Affairs of the Republic of Indonesia. “Indonesia dan Negara-Negara Afrika Tandatangani MoU Industri Strategis di IAF 2024.” September 3, 2024. https://kemlu.go.id/berita/indonesia-dan-negara-negara-afrika-tandatangani-mou-industri-strategis-di-iaf-2024.

Ministry of Defense of the Republic of Indonesia. “Unhan RI Sukses Luncurkan Satelit Nano Indonesia, RIDU-Sat 1.” June 25, 2025. https://www.kemhan.go.id/2025/06/25/unhan-ri-sukses-luncurkan-satelit-nano-indonesia-ridu-sat-1.html.

Keselman, Gene, and Fiona Murray. “Dual-Use Is a Strategy, Not a Category (Nor a Trap).” *War on the Rocks*, January 2, 2025. https://warontherocks.com/dual-use-is-a-strategy-not-a-category-nor-a-trap/.

Defense Industry Policy Committee (KKIP). “Rencana Aksi Industri Pertahanan: Penguasaan Sepuluh Teknologi Prioritas.” February 20, 2023. https://www.kkip.go.id/2023/02/20/rencana-aksi-industri-pertahanan-penguasaan-sepuluh-teknologi-prioritas/.

———. “Sejarah Industri Pertahanan Nasional.” https://www.kkip.go.id/sejarah.

Kompas.com. “Kemenhan Bentuk Badan Baru, Diminta Pastikan Tidak Ada Tumpang Tindih.” August 8, 2025. https://nasional.kompas.com/read/2025/08/08/20124741/kemenhan-bentuk-badan-baru-diminta-pastikan-tidak-ada-tumpang-tindih.

Kompas.id. “Kadispenad: Kontrak Monitoring Medsos Rp 49,2 Miliar Tidak Pernah Dilaksanakan.” April 30, 2026. https://www.kompas.id/artikel/kadispenad-kontrak-monitoring-medsos-rp-492-miliar-tidak-pernah-dilaksanakan.

———. “Publik Pertanyakan Anggaran Rp 49,2 Miliar untuk Monitoring Medsos TNI AD.” April 29, 2026. https://www.kompas.id/artikel/anggaran-rp-492-miliar-untuk-monitoring-medsos-tni-ad-dipertanyakan-publik.

Kuntsman, Adi, and Rebecca L. Stein. *Digital Militarism: Israel’s Occupation in the Social Media Age*. Redwood City: Stanford University Press, 2015.

Lamensch, Marie. “Authoritarianism Has Been Reinvented for the Digital Age.” Center for International Governance Innovation, 9 July 2021. https://www.cigionline.org/articles/authoritarianism-has-been-reinvented-for-the-digital-age/.

Lassman, Thomas C. “Putting the Military Back into the History of the Military-Industrial Complex: The Management of Technological Innovation in the US Army, 1945–1960.” Isis 106, no. 1 (2015): 94–120. https://doi.org/10.1086/681038.

Ledbetter, James. *Unwarranted Influence: Dwight D. Eisenhower and the Military-Industrial Complex*. New Haven, CT: Yale University Press, 2011.

Liang, Xiao, Nan Tian, Diego Lopes da Silva, Lorenzo Scarazzato, Zubaida Karim, and Jade Guiberteau Ricard. “Trends in World Military Expenditure, 2025.” *SIPRI Fact Sheet*. Stockholm International Peace Research Institute (SIPRI), April 2026.

Lindsey, Tim. “Indonesia’s New President, Prabowo Subianto, Finds Democracy ‘Very Tiring’. Are Darker Days Ahead for the Country?” *The Conversation*, 18 October 2024.

https://theconversation.com/indonesias-new-president-prabowo-subianto-finds-democracy-very-tiring-are-darker-days-ahead-for-the-country-241256.

Loewenstein, Antony. *The Palestine Laboratory: How Israel Exports the Technology of Occupation Around the World*. London: Verso, 2023.

Lopes, Gonçalo. "From Orbit to Cyber Wars: The New Era of Civil-Military Synergy." *VisionSpace*, March 25, 2025. https://visionspace.com/from-orbit-to-cyber-wars-the-new-era-of-civil-military-synergy/.

LP3ES. "Membangun Resiliensi Masyarakat Sipil Setelah 27 Tahun Reformasi." May 22, 2025. https://www.lp3es.or.id/2025/05/22/membangun-resiliensi-masyarakat-sipil-setelah-27-tahun-reformasi /.

Luckey, David, et al. *Measuring Intelligence, Surveillance, and Reconnaissance Effectiveness at the United States Central Command*. Santa Monica, CA: RAND Corporation, 2021.

Lyon, David. *The Culture of Surveillance: Watching as a Way of Life*. Cambridge: Polity Press, 2018. https://www.perlego.com/book/1536337/the-culture-of-surveillance-watching-as-a-way-of-life-pdf.

Macaluso, Alyssa. "Space Is Not a Human Rights Vacuum." Science & Politics, 25 February 2026. https://sciencepolitics.org/2026/02/25/space-is-not-a-human-rights-vacuum/.

Mambrini, Tommaso. "Dual-Use Technologies in the Rise of the Space Economy." *Berkeley Technology Law Journal*, April 28, 2026. https://btlj.org/2026/04/dual-use-technologies-in-the-rise-of-the-space-economy/.

Mann, Tim. "Activists on Trial: The Weaponization of Online Defamation Provisions in Indonesia." *Australian Journal of Asian Law* 25, no. 2 (2025): 1–16.

Mantalean, Vitorio, and Ardito Ramadhan. "Imparsial: Pengadaan Alutsista Rawan Korupsi dengan Dalih Rahasia Pertahanan." *Kompas.com*, December 10, 2024.

Mathe, Zen, and Caryn Dolley. "Unaccountable 0004: Rheinmetall Denel Munition: Murder and Mayhem in Yemen." *Open Secrets*, January 22, 2020. https://www.opensecrets.org.za/rheinmetall-denel-munition-murder-and-mayhem-in-yemen/.

McConnell, B. "How Cyberspace Is at the Leading Edge of Global Change." *The Diplomat*, February 25, 2016. https://thediplomat.com/2016/02/how-cyberspace-is-at-the-leading-edge-of-global-change.

Mengko, Diandra Megaputri, and Aulia Fitri Rosadi. "Non-Institutionalized Civilian Control and Military Operations Other than War in Indonesia." In *Military Modernization and Civil-Military Relations in Indone*sia, edited by Muhamad Haripin, Adhi Priamarizki, and Leonard C. Sebastian. Singapore: Palgrave Macmillan, 2025.

Michaelsen, Marcus. *The Digital Transnational Repression Toolkit, and Its Silencing Effects*. Freedom House, 2020. https://freedomhouse.org/report/special-report/2020/digital-transnational-repression-toolkit-and-its-silencing-effects.

Mietzner, Marcus. "The Military's Transformation from Praetorian Ruler to Presidential Coalition Partner." In *Oxford Research Encyclopedia of Politics*, edited by Erin Hannah. New York: Oxford University Press, 2020.

Miller, Seumas. *Dual Use Science and Technology, Ethics and Weapons of Mass Destruction*. Cham: Springer, 2018.

Ministry of Foreign Affairs of Pakistan. “Joint Statement by the Foreign Ministers of Jordan, United Arab Emirates, Indonesia, Pakistan, Turkey, Saudi Arabia, Qatar and Egypt.” https://mofa.gov.pk/press-releases/joint-statement-by-the-foreign-ministers-of-jordan-united-arab-emirates-indonesia-pakistan-turkiye-saudi-arabia-qatar-and-egypt.

Mills, C. Wright. *The Power Elite*. New York: Oxford University Press, 1956.

MIT Mission Innovation X (MIx). “Defining ‘Dual-Use.’“ *Dual-Use Readiness Model*. https://dualuse.mit.edu/defining-dual-use/.

Muir, Laura. “Control Space?: Cinematic Representations of Surveillance Space between Discipline and Control.” *Urban Surveillance* 9, no. 3 (2012): 263–279.

Munthaha, Dwi. “Militer Era Prabowo: Pretorianisme Baru?” *Kompas.id*, August 20, 2025. https://www.kompas.id/artikel/militer-era-prabowo-pretorianisme-baru.

NATO. *Summary of NATO’s Revised Artificial Intelligence (AI) Strategy*. July 10, 2024. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy.

Neumann, Isabella. “It Is Complicated: Cyber into the Civil–Military Relationship.” *Journal of Cybersecurity* 12, no. 1 (2026): 1–12. https://doi.org/10.1093/cybsec/tyag012.

New Internationalist. “How Palestine Became Israel’s Spyware Test-Bed.” https://newint.org/features/2023/10/02/spy-games.

Ni Aoláin, Fionnuala, and Adriana Edmeades Jones. “Spyware Out of the Shadows: The Need for a New International Regulatory Approach.” *Just Security*, May 16, 2023. https://www.justsecurity.org/86558/spyware-out-of-the-shadows-the-need-for-a-new-international-regulatory-approach/.

Ní Aoláin, Fionnuala. *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach*. Position papers. Geneva: Office of the United Nations High Commissioner for Human Rights, April 2023. https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf.

Niiles, Sofia. “Dual-Use Satellites and the Law of Armed Conflict: The Tension Between Targeting Rules and State Responsibility in Outer Space.” *Amsterdam Law Forum*, 10 June 2026. https://vu.nl/en/news/2026/dual-use-satellites-and-the-law-of-armed-conflict.

Nugraha, Taufik Rachmat, and Bich Tran. *Bridging the Legal and Strategic Mismatch in the Indonesian Air Force’s Space Unit*. IDSS Paper IP26100. Singapore: S. Rajaratnam School of International Studies, Nanyang Technological University, August 27, 2026. https://rsis.edu.sg/rsis-publication/idss/ip26100-bridging-the-legal-and-strategic-mismatch-in-the-indonesian-air-forces-space-unit/.

Office of the United Nations High Commissioner for Human Rights (OHCHR). “UN Experts Condemn ‘Board of Peace,’ Call for a Reparative, Rights-Based Approach to Reconstruction in Gaza.” https://www.ohchr.org/en/special-procedures/sr-housing/mr-balakrishnan-rajagopal.

———. Special Procedures. “Communication to Rheinmetall AG.” Ref. AL OTH 81/2024. 17 May 2024. https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=29 082.

Peron, AE dos R., D. Almstadter Mattar de Magalhães, and GF Caetano. “Beyond Digital Repression: Techno-Authoritarianism in Radical Right Governments.” *Cogent Social Sciences* 11, no. 1 (2025). https://doi.org/10.1080/23311886.2025.2528457.

Piovesan, Giorgia. “Digital Authoritarianism in the Middle East.” *The Security Distillery*, April 19, 2023. https://thesecuritydistillery.org/all-articles/digital-authoritarianism-in-the-middle-east.

Poetranto, Irene. “Techno-Legal Internet Controls in Indonesia and Their Impact on Free Expression.” In *Digital Democracy in a Divided Global Landscape*, 35–38. Washington, DC: Carnegie Endowment for International Peace, 2025.

———. “The Architecture of Digital Repression: Internet Service Providers Can Facilitate Internet Access but Also Draconian Control.” *Carnegie Endowment for International Peace*, March 10, 2026. https://carnegieendowment.org/research/2026/03/the-architecture-of-digital-repression.

Polyakova, Alina, and Chris Meserole. *Exporting Digital Authoritarianism: The Russian and Chinese Models*. Washington, DC: Brookings Institution, 2019.

Priamarizki, Adhi, and Edna Caroline. *Prabowo’s Defense Challenge: Making the “Triple Helix” Work*. IDSS Paper IP26067. Singapore: S. Rajaratnam School of International Studies, Nanyang Technological University, 21 May 2026. https://rsis.edu.sg/rsis-publication/idss/ip26067-prabowos-defence-challenge-making-triple-helix-work/.

Privacy International. “Challenging the Militarisation of Tech.” https://privacyinternational.org/campaigns/militarisation-of-tech.

———. “State of Privacy: Egypt.”January 26, 2019. https://www.privacyinternational.org/state-privacy/1001/state-privacy-egypt.

———. “What Is Militarisation of Tech? ” September 12, 2025. https://privacyinternational.org/long-read/5668/what-militarisation-tech.

Privacy International and ELSAM. *Privasi 101: Panduan Memahami Privasi, Perlindungan Data, dan Surveilans Komunikasi*. Jakarta: ELSAM and Privacy International, 2015.

Privacy International and PAX. *Tech Giants, the Arms Industry and the Weaponization of AI: When Algorithms Go to War*. June 2026.

Priyandita, Gatra, and Christian Guntur Lebang. “Indonesia’s Cyber Soldiers: Armed without a Compass.” *The Strategist*, April 11, 2025. https://www.aspistrategist.org.au/indonesias-cyber-soldiers-armed-without-a-compass/.

Probasco, Emelia, Helen Toner, Matthew Burtell, and Tim GJ Rudner. “AI for Military Decision-Making: Harnessing the Advantages and Avoiding the Risks.” *Center for Security and Emerging Technology*, April 2025. https://doi.org/10.51593/20240028.

PT Dahana. “Dahana–RDM Sepakati Pembangunan Fasilitas Energetic Material di Indonesia.” November 25, 2025. https://dahana.id/id/dahana-rdm-sepakati-pembangunan-layanan-energetic-material-di-indonesia/.

PT Pindad (Persero). “Pindad Bersiap Menjadi Produsen Munisi Globa.” August 8, 2014. https://pindad.com/pindad-bersiap-menjadi-produsen-munisi-global.

———. “Kendarai Ranops Maung, Presiden Tinjau Divisi Munisi dan Apresiasi Kemampuan Lini Produksi PT Pindad.” July 27, 2023. https://pindad.com/kendarai-ranops-maung-presiden-tinjau-divisi-munisi-dan-apresiasi- mampu-lini-produksi-pt-pindad.

Rafiq, Aamna. “Militarization of Artificial Intelligence and the Future of Arms Control in South Asia.” *Strategic Studies* 41, no. 2 (2021): 49–63.

Rahmawati, Dwi. “Bahas Anggaran Kemhan 2025, Rapat Komisi I DPR Digelar Tertutup.” *detikNews*, June 12, 2024. https://news.detik.com/berita/d-7386957/bahas-anggaran-kemhan-2025-rapat-komisi-i-dpr-digelar-tertutup.

Rakhmat, Muhammad Zulfikar. “Indonesia Cannot Condemn Gaza Genocide While Still Silent on Its Use of Israel Spyware.” *Middle East Monitor*, September 30, 2025. https://www.middleeastmonitor.com/20250930-indonesia-cannot-condemn-gaza-genocide-while-still-silent-on-its-use-of-israeli-spyware/.

Remanu, Alifah Jasmine Kallista, Calista Sahlah Purwanto, Nadhira Nurul Fajri, and Firman. “Analisis Implikasi UU ITE terhadap Kebebasan Berekspresi di Ruang Digital: Studi Kasus Greenpeace Indonesia.” *ISO Journal: Journal of Social, Political and Humanitarian Sciences* 4, no. 2(2024).

Reporters Without Borders (RSF). “Egypt’s New Cybercrime Law Legalizes Internet Censorship.” August 21, 2018. https://rsf.org/en/egypt-s-new-cybercrime-law-legalizes-internet-censorship.

Reuters. “Indonesian Officials Targeted by Spyware: Sources.” *Al Jazeera*, 30 September 2022. https://www.aljazeera.com/economy/2022/9/30/indonesian-officials-targeted-by-spyware-sources.

Riecke, Lena. “Unmasking the Term ‘Dual Use’ in EU Spyware Export Control.” *European Journal of International Law* 34, no. 3 (2023): 697–720. https://doi.org/10.1093/ejil/chad039.

Rheinmetall. “Rheinmetall Denel Munition (Pty) Ltd.” https://www.rheinmetall.com/en/company/subsidiaries/rheinmetall-denel-munition.

Ritonga, Machradin Wahyudi. “Dinilai Cederai Demokrasi, Wewenang TNI dalam RUU Keamanan dan Ketahanan Siber Jadi Sorotan.” *Kompas.id*, October 4, 2025. https://www.kompas.id/artikel/dinilai-cederai-demokrasi-wewenang-tni-dalam-ruu-cybersecurity and resilience in the spotlight.

Rogers, James Patton. “Introduction: Why Study Drones?” In *De Gruyter Handbook of Drone Warfare*, edited by James Patton Rogers, 1–? Berlin/Boston: De Gruyter, 2024.

Romero, Gina. Pro*tecting the Right to Freedom of Peaceful Assembly and Association from Stigmatization*. Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association. UN Doc. A/79/263. United Nations, 31 July 2024. https://digitallibrary.un.org/record/4059940/files/A_79_263-EN.pdf.

———. *Unmasking the Chilling Effects of the Digital Surveillance Ecosystem: The Erosion of Assembly and Association Rights*: Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and Association. A/HRC/62/45. Geneva: United Nations, 21 April 2026. https://digitallibrary.un.org/record/4113878.

Rosner, Robert. “Preface.” In *Governance of Dual-Use Technologies: Theory and Practice*, edited by Elisa D. Harris. Cambridge, MA: American Academy of Arts and Sciences, 2016.

Saraçoğlu, Diyar. “From Productive Force to Destructive Force: Digital Colonialism in Palestine.” bianet, 7 October 2025. https://bianet.org/yazi/from-productive-force-to-destructive-force-digital-colonialism-in-palestine-312332.

Schäfer, Saskia, and Daniel Peterson. “Appropriations of Human Rights Discourses: Evidence from Indonesia and Malaysia.” *International Journal of Constitutional Law* 24, no. 1 (January 2026).

Setiawan, Ken MP, “A State of Surveillance? Freedom of Expression under the Jokowi Presidency.” In *Democracy in Indonesia: From Stagnation to Regression?* edited by Thomas Power and Eve Warburton. Singapore: ISEAS–Yusof Ishak Institute, 2020.

Shaheen, Rubina. “Gender and Surveillance: The Implications of Biometric Technologies for Privacy and Equity.” *Journal of Gender, Power, and Social Transformation* 1, no. 3 (2024).

Shin, Beomchul. *The Republic of Korea’s Perspective on Defense Transparency*. Policy Brief No. 2011-1. Northeast Asia Defense Transparency Project, University of California Institute on Global Conflict and Cooperation, October 2011.

Shpak, Valerij. “Indirect Praetorianism: The Case of Turkey’s Military.” *Scientific Journal of the Military University of Land Forces* 54, no. 4(206) (2022): 624–638. https://doi.org/10.5604/01.3001.0016.0757.

Sinha, Bappa. “Big Tech’s Deep Links with Genocide in Gaza.” *NewsClick*, 6 October 2025. https://www.newsclick.in/big-techs-deep-links-genocide-gaza.

South China Morning Post. “Facial Recognition Is Used in China for Everything from Refuse Collection to Toilet Paper Dispensers and Its Citizens Are Increasingly Alarmed, Survey Shows.” 2021. https://www.scmp.com/tech/innovation/article/3119281/facial-recognition-used-china-everything-refuse-collection-toilet.

Southeast Asia Freedom of Expression Network (SAFEnet). *Laporan Situasi Hak-hak Digital Indonesia 2020: Represi Digital di Tengah Pandemi*. Denpasar: Southeast Asia Freedom of Expression Network (SAFEnet), 2021.

———. “Pernyataan Sikap SAFEnet: Tolak RUU TNI, Tolak Militerisasi Ruang Siber.” March 17, 2025. https://safenet.or.id/id/2025/03/tolak-ruu-tni-tolak-militerisasi-ruang-siber/.

Stelpflug, Timo. “The Resurgence of European and UK Defense Tech: Markets, Technology, and Investment.” *Taylor Wessing*, July 31, 2025. https://www.taylorwessing.com/en/interface/2025/defence-tech/the-resurgence-of-european-and-uk-defence-tech.

Stockholm International Peace Research Institute (SIPRI). “Unprecedented Rise in Global Military Expenditure as European and Middle East Spending Surges.” Press Release, 28 April 2025. https://www.sipri.org/media/press-release/2025/unprecedented-rise-global-military-expenditure-european-and-middle-east-spending-surges.

Tangredi, Sam J., and George Galdorisi, eds. *AI at War: How Big Data, Artificial Intelligence, and Machine Learning Are Changing Naval Warfare*. Annapolis, MD: Naval Institute Press, 2021.

Tempo. “Cerita Kepala Desa soal Peran Tentara di Kopdes Merah Putih.” February 16, 2026. https://www.tempo.co/politik/cerita-kepala-desa-soal-peran-tentara-di-kopdes-merah-putih-2115459.

———. “Demokrasi Santun Prabowo Subianto.” October 23, 2024. https://www.tempo.co/kolom/demokrasi-santun-prabowo-subianto-1096274.

———. “Jokowi Pamer Pegang Data Intelijen Arah Parpol, Begini Bunyi Pasal 1 dan 2 UU Nomor 17 Tahun 2011 tentang Intelijen Negara.” September 20, 2023.

https://www.tempo.co/politik/jokowi-pamer-pegang-data-intelijen-arah-parpol-begini-bunyi-pasal-1-dan-2-uu-nomor-17-tahun-2011-tentang-intelijen-negara-141871.

———. “Koperasi Desa Merah Putih.” Tempo.co. https://www.tempo.co/tag/koperasi-desa-merah-putih.

———. “Menhan: Kebutuhan Anggaran Pertahanan Tahun 2027 Rp 667 Triliun.” https://www.tempo.co/politik/menhan-kebutuhan-anggaran-pertahanan-tahun-2027-rp-667-triliun-2266159.

Tempo Editorial. “The Dark Threat of Surveillance Equipment.” *Tempo.co*, 9 May 2024. https://en.tempo.co/read/1865183/the-dark-threat-of-surveillance-equipment.

Tian, Nan, and Xiao Liang. *Rebalancing Military Spending Towards Achieving Sustainable Development*. SIPRI Research Policy Paper. Stockholm: Stockholm International Peace Research Institute (SIPRI), November 2025. https://doi.org/10.55163/ZCIE5196.

US Central Command. “About Us.” https://www.centcom.mil/ABOUT-US/.

US Department of Defense. “Project Maven Industry Day Pursues Artificial Intelligence for DoD Challenges.” November 3, 2017.

———. “Project Maven to Deploy Computer Algorithms to War Zone by Year’s End.” July 21, 2017.

Ufen, Andreas. “The Rise of Digital Repression in Indonesia under Joko Widodo.” *GIGA Focus Asia*, no. 1 (January 2024). https://doi.org/10.57671/gfas-24012.

UN B-Tech Project, Heartland Initiative, Business & Human Rights Resource Center, and Open MIC. “Key Takeaways: Dual-Use Dominance When Every Innovation Has a Defense Application.” July 26, 2025. https://www.ohchr.org/sites/default/files/documents/form/defense-application-key-takeaways-25-internet-governance-forum-side-event-dual-use-dominance-innovation-1-en.pdf.

United Nations. Secretary-General. *The Security We Need: Rebalancing Military Spending for a Sustainable and Peaceful Future*: Report of the Secretary-General on the Impact of the Global Increase in Military Expenditure on the Achievement of the Sustainable Development Goals as Requested by Action13(c) of the Pact for the Future.2025. https://digitallibrary.un.org/record/4088022/files/SG_Report_TheSecurityWeNeed.pdf.

University World News. “Indonesia Ramps Up R&D Space to Reduce Foreign Reliance.” November 25, 2025. https://www.universityworldnews.com/post.php?story=20251125121827251.

Vaseashta, Ashok, and Alvaro Rocha, eds. *Spectrum of Dual-Use Technologies: Unforeseen Risks Versus Returns*. Cham: Springer Nature Switzerland, 2026. https://doi.org/10.1007/978-3-032-00202-0.

VOA Indonesia. “Perketat Pengawasan, Junta Myanmar Pasang CCTV Canggih China di Lebih Banyak Kota.” July 7, 2022. https://www.voaindonesia.com/a/perketat-pengawasan-junta-myanmar-pasang-cctv-canggih-china-di-lebih-banyak-kota-/6653414.html.

War on Want. “Israeli Spyware Is Threatening Our Rights and Freedoms.” https://waronwant.org/resources/israeli-spyware-threatening-our-rights-and-freedoms.

Waters, Nick. “First ISIS, then Iraq, now Israel: IDF Use of Commercial Drones.” *Bellingcat*, 18 June 2018. https://www.bellingcat.com/news/middle-east/2018/06/18/first-isis-iraq-now-israel-idf-use-commercial-drones/.

Widyatama, Elvan. “Gila-Gilaan! AS Habiskan Rp6.000 T Buat Teknologi Perang Masa Depan.” CNBC Indonesia, November 13, 2025. https://www.cnbcindonesia.com/research/20251112105824-128-684492/gila-gilaan-as-habiskan-rp6000-t-buat-teknologi-perang-masa-depan.

Wijayanto. “Masyarakat Sipil dan Represi Digital.” *Kompas*, June 10, 2025. https://www.kompas.id/artikel/melindungi-masyarakat-sipil-dari-represi-digital-2.

Willoughby, Angus. “Biometric Surveillance and the Right to Privacy.” October 5, 2017. https://technologyandsociety.org/biometric-surveillance-and-the-right-to-privacy/.

Wingender, Asger Mose, and Søren Bang. “Modern Arms Technologies Help Autocratic Rulers Stay in Power.” University of Copenhagen, January 25, 2023. https://news.ku.dk/all_news/2023/01/modern-arms-technologies-help-autocratic-rulers-stay-in-power.

Withrington, Claire. “The Internet of Military Things.” August 24, 2023. https://cove.army.gov.au/article/internet-military-things.

Yilmaz, Ihsan, Ali Mamouri, Shahram Akbarzadeh, and Muhammad Omer. *Authoritarian Diffusion in the Cyberspace: How Egypt Learns, Emulates, and Cooperates in Digital Authoritarianism*. Brussels: European Center for Populism Studies, 2025. https://doi.org/10.55271/rp0097.

Yousef, Mohammad. “Why the Recent UNSC Resolution 2803 ‘Board of Peace’ Violates the UN Charter.” *Middle East Monitor*, November 21, 2025. https://www.middleeastmonitor.com/20251121-why-the-recent-unsc-resolution-2803-board-of-peace-violates-the-un-charter/.

Since its founding on August 14, 1993, the Institute for Policy Research and Advocacy (ELSAM) has developed a strategy to combine the working methods of think tanks and human rights movements in its operations. This characteristic makes ELSAM unique as a movement-based think tank, with two main focuses: studies using a rights-based approach and policy advocacy. ELSAM strives to continuously promote evidence-based policies to strengthen respect for, fulfillment of, and protection of human rights.

The establishment of ELSAM is intended to achieve the goal of realizing a social order that adheres to the values of human rights, justice and democracy. In achieving this goal, ELSAM develops at least four main activities: (1) the study and production of human rights knowledge to support policy advocacy; (2) mainstreaming human rights in policy formation; (3) legal advocacy to encourage policy change, including through strategic litigation; and (4) organizing various human rights education programs, with a variety of topics and diverse target audiences.

The various main activities above are mainly applied in a number of ELSAM strategic topic areas, which focus on the issues of: (1) Human Rights and Technology, especially responding to the speed of digital technology innovation that has a broad impact on human rights; (2) Human Rights and Business, considering the increasing role of corporations in influencing the relationship between rights holders and obligation holders; (3) Human Rights and the Environment, the importance of emphasizing environmental sustainability as part of human rights; (4) Basic Freedoms, especially freedom of expression, freedom of religion/belief, and freedom of assembly/association; (5) Transitional Justice, efforts to encourage the completion and accountability of various crimes against human rights in the past. For more than two decades ELSAM has made a number of contributions in encouraging the adoption and implementation of human rights in Indonesia, starting from the ratification of various international human rights conventions, to the formation of a number of laws. Various laws that were born after the reformation, such as the Truth and Reconciliation Commission Law, the Witness and Victim Protection Law, and most recently the Personal Data Protection Law, ELSAM was specifically involved in the formation process.

In its current development, ELSAM is pushing for various policies to respond to the rapid pace of digital technology innovation. ELSAM's contribution to delivering digital policies that emphasize a human-centric approach was publicly recognized with its recognition as the winner of the 2020 Good ID Award in the security category. This global award recognizes individuals and civil society organizations that make significant contributions to promoting good digital policies.

ELSAM is also actively involved in strengthening human rights institutions in Indonesia, such as the National Human Rights Commission (Komnas HAM), the Witness and Victim Protection Agency (LPSK), and ensuring consistent human rights implementation through support for optimizing the National Action Plan (RAN) for Human Rights. ELSAM also continuously strengthens the capacity of various human rights stakeholders, both state and civil society. ELSAM conducts human rights courses on various topics for human rights defenders, public lawyers, policymakers, law enforcement officials, and corporations.

Towards 2045, ELSAM has a final goal of change: "An empowered, inclusive, equal, and technologically proficient Indonesian society within a human rights and democratic order for

social and ecological justice." Translated in the 2025-2030 Strategic Plan which is divided into 5 (five) Intermediate Outcomes, as follows:

1. Building the foundation for a political alliance with reformers in state institutions.
2. Strengthening the critical perspective of civil society on policies in the context of the digital universe.
3. Availability of knowledge infrastructure to foster human rights activism in the digital universe.
4. The development of a new constituency with a human rights perspective as citizens in the digital universe.
5. The development of a new narrative that supports the human rights agenda and victims' rights in the digital universe.

Address:

Jl. Siaga II No. 31, Pasar Minggu, Jakarta 12510 INDONESIA

Phone: (+62 21) 797 2662

Email: office@elsam.or.id

Website: www.elsam.or.id

Social media:

X: @elsamnews Instagram: @elsamnews Facebook: @elsamjkt Youtube: @perkumpulanelsam