Innováció

HM Electronics, Logistics and Property Management Ltd. Volume 4, Issue 2 | 2026

Responsible publisher

	Contacts	
Postal address	1101 Budapest, Salgótarjáni street 20.	HM EI Ltd. Competence Centre
Mobile	Dr. István Kobolka	+36 30 979 6128
E-mail	kobolka.istvan@hmei.hu einnovacio@hmei.hu	

Printing: The MoD Zrínyi Geoinformation and Recruitment Support Public Benefit Non-profit Ltd.
2026
Responsible Manager: Zoltán Pásztor Director

ISSN 2939-7677

Tibor Szilvágyi (PhD) Dr.[1]:

Thoughts on the future robotic warfare – Misconceptions and challenges

Abstract:

Robotic warfare is an ultramodern future method of waging a war that slowly but unstoppable approaches to the reality. Disruptive technologies, among others remotely guided and autonomous weapons systems as well as swarm and artificial intelligence fuel this process, which is paved by many difficulties, misconceptions and challenges. The elaborated PESTEL analysis helps us to understand the requirements and the environment of the debated robotic warfare, which aspires to be sustainable and less destructive while requiring huge human, material and technological resources. Giving the decision-making authority to autonomous machines raises serious ethical and security issues, international organisations should deal with. This publication aims to draw the attention to a controversial phenomenon, the coveted development of military robotics and its possible harmful consequences.

Keywords: robotic warfare, disruptive technologies, unmanned aircraft systems, unmanned ground vehicles, artificial intelligence, swarm operation, military robots, autonomous weapons systems, PESTEL analysis, misconception, security challenge

Introduction

Nobody is able to predict near-term international security policy events and challenges since these are influenced by many, unforeseeable aspects. The only certain thing is that the future in many regions of the world is uncertain. International relations are always changing according to the will and interests of main actor states, mainly the global great powers. In the second quarter of the 21st century realism is again overwhelming idealism that increases the possibilities of rhetorical and violent confrontations among opposing players, mainly nation-states. There are two actual and most influential examples: the Russian–Ukrainian military conflict (invasion launched on the 24th of February 2022) and the Israeli–American strikes against Iran (started on the 28th of February 2026).

War as a weird phenomenon and its varieties have always been in the centre of historical events. Tragedies and enlightenments have usually been following each

[1] Project leader at the Aviation Division of the Electronics and Informatics Directorate of the Electronics, Logistics and Property Management Company Limited by Shares (HM EI Zrt.).

other and a similar situation is repeating itself even nowadays. The famous military scientist, Carl von Clausewitz (1780–1831) was dealing with the nature of war and finally stated in his oeuvre (*On War* – in German: *Vom Kriege*) that "War is a mere continuation of policy by other means."[2] If we accept this statement as a valid truth today, we have to think about the nature of politics as well. Similar to Clausewitz's statement, in my opinion the politics might be the continuation of a war with other means as well. Wars and politics have the same goal, namely protecting the interests of an entity but with different means. Since war is one of the tools asserting the interests of a nation or an organisation, we have to research its forms and their consequences as well. War and politics are inseparable from each other and both are interdependent in a so-called historical circle.

Current strategists often think and speak about a future robotic warfare that will be totally different from the earlier military confrontations and conflicts. Fortunately, we have not reached this stage yet. The recent Russian–Ukrainian armed conflict is a combination of the old and new school of military operations. It started with conventional weapons and methods in 2022 and shortly returned to a hybrid combat format. Even the early March 2026 Israeli–American airstrikes against Iran and their counter acts were also far away from a modern robotic warfare. Reading this publication until the end, we will see why.

My estimation and hypotheses are that a pure robotic warfare is so futuristic that now we are not able to imagine and predict its possible forms and features. It develops continuously. The current chance is very little to have a war or military conflict exclusively waged by robots and advanced autonomous military technology. The human being should always be in the loop (direct influence) or on the loop (supervising the happenings), otherwise it will be only a military technology competition or race between and among states.

Recently international stability, security and order have become more and more complex, complicated and vulnerable. Now the world's multifaceted processes and their consequences are not easy to understand. This is the reason, why many (political and military) leaders are not able to make proper decisions. Their reactions to certain strategic happenings are sometimes uncommon, excessive and outrageous. Their behaviour can be evaluated as a kind of a cognitive dissonance phenomenon well-known in the psychology.[3] This cognitive controversy causes that sometimes these political leaders act just the opposite they should have done.

Warfare might be directed to gain territorial, economic or political assets. Every war or military conflict needs different strategy, human resources, military technology and infrastructure. These are influenced by the capabilities and strategy of the

[2] Clausewitz: War as Politics by other Means; https://oll.libertyfund.org/pages/clausewitz-war-as-politics-by-other-means Downloaded: 19. April 2026

[3] Cognitive dissonance is the mental discomfort experienced when a person holds two conflicting beliefs or when their actions don't align with their beliefs. To reduce this uncomfortable feeling, people often change their thoughts or justify their behaviour to make everything feel more consistent. What Is Cognitive Dissonance Theory? https://www.simplypsychology.org/cognitive-dissonance.html Downloaded: 19. April 2026

enemy; the own political, economic, social and military resources; and the whole, complex geopolitical situation. Belligerents usually wage the war not independently but in tight or loose coalition with allies and apply all their tools and capacities available for this purpose. Strategy should be a serious and long-term program and not a daily baseless rumour as we experience it in many cases today.

Now let's speak about robotic warfare that is worth analysing and assessing before we make final statements about it.

Meaning of the robotic warfare

The robotic warfare directly means that robots (mainly remotely guided and autonomous weapons systems) are fighting against each other and human beings only check and follow the military events. The current technology makes it possible that weapons systems can work pre-programmed automatically or autonomously with the support of artificial intelligence (AI). So, we can think that wars in the future might be waged without soldiers but this is a huge misunderstanding. As for my estimation a complete robotic warfare (Figure 1) is not realistic in the foreseeable future, but in short-term we will see its initial marks.

The current development of warfare shows a much bigger role of automatic and autonomous solutions in weapon systems than during earlier military confrontations. In the history we can find evidence how tanks, airplanes and missiles were able to amend the ideology of warfare and also the whole military strategy of a country depending on its real geopolitical situation. The former Soviet Union was believing in the hegemony of Land Forces, mainly their tanks and artilleries. The United States (US) and the United Kingdom as main see powers have developed firstly their Navy and Air Force. Missiles with warheads have become an ultimate weapon for every global great power (US, China, Russia), especially when these are equipped with nuclear payload. Nuclear weapon remains a deterrent tool that plays a strong restraining force. However, we can state that conventional weapon systems further will have an enormous role in wars and military conflicts but information technology (IT) determines more and more the modern warfare than old military hardware.[4]

Humanists unfoundedly expect from the robotic warfare that these robotised military conflicts will be hopefully less destroying and more human than earlier armed airstrikes and ground or naval operations. According to their beliefs, with using precise weapons and ammunitions civilians might be saved from collateral damages and from humanitarian catastrophe. However, I can state that military confrontations will never be human neither in the near, nor in the far future. If we analyse the armed conflicts in the last centuries, we can estimate that these violent acts are

[4] George and Meredith Friedman: Future of War – Power, technology and American world dominance in the twenty-first century; St. Martin's Griffin, New York, 1996; ISBN 0-312-18100-0; Part 1: Weapons and Strategy (Introduction: The Culture of War and 1 David's Sling: On the Rise and Fall of Weapons; p 15–38

Image 1: Fantasy about robotic warfare; Thomas Anglero: The Future of Warfare: How AI and Robotics Are Redefining Global Security; March 19, 2025; https://www.anglero.com/2025/03/19/future-of-warfare-how-ai-and-robotics/ Downloaded: 18. April 2026

enough and will be more and more brutal that are made by human beings (terrorists, soldiers and politicians) and directed very often against innocent people. Faith in the sense of a war depends on people (mainly citizens and voters) who are for or against the fights and hostilities. For example, according to three public surveys conducted in March 2026, the Israel Democracy Institute published the poll results in which the Israeli Jewish public support for the American–Israeli Operation Roaring Lion (in the United States: Operation Epic Fury) against Iran still had a large majority (78%) at the end of March 2026. However, the share of those Jewish persons, who opposed the operation, has risen from 4% in the two previous surveys to 11.5% in the last one. There has also been a clear decline in the strength of support. The proportion of Jewish citizens who strongly support the operation dropped from 74% at the beginning of March when fighting began to 68% mid-month and to just 50% at the end of the month. Only a small minority of Arab respondents supports the operation and this share has also declined from roughly one-quarter (26% and later 25%) in earlier measurements to 19% at the end of March. In the total sample, the level of support stands at 68%, though this largely represents the views of the Jewish respondents, due to their numerical superiority over the Arab population.[5]

Average people might think that humanoid robots can replace soldiers and that way we can avoid human casualties in the military field but this seems to be also no realistic. Fighting would lose its original meaning if human beings fall out from this circle. Unfortunately, the outcome of wars always depends on the casualties and sufferings of humans that put pressure on the opposing parties' political and mili-

[5] Prof. Tamar Hermann, Dr. Lior Yohanani, Yaron Kaplan: Most Jewish Israelis Think PM Netanyahu's Motivation in the War is Security Related; Most Arabs Think It's Personal; 30 March 2026; https://en.idi.org.il/articles/63856 Downloaded: 19. April 2026

tary leaders. The longitude of a war or military conflict is mainly influenced by the emotional, political and economic resilience of the society in a participant country. It is also unambiguous that the pain threshold of a nation is different in democratic and autocratic countries. Everybody can imagine which is more resilient (autocracy) and which is more sensible (democracy) in this case.

A robotic warfare is not a general one. It has several developing stages or levels where robotics and autonomous technology as well as their measures are in different proportions in the so-called hybrid (conventional and most advanced at the same time) content. It might be a low, a medium and a high-level robotic warfare but a complete one is not real. Robotic warfare categories should be worked out by strategists in the future. This is not the aim of this publication.

Remotely controlled and autonomous military robots and weapons

Military robots are such kinds of machines that perform defence-related tasks with limited or no direct human intervention. The most important feature of their activities is that they have no human physiological limitations since on their board there is no crew. These systems use advanced sensors, have secure communication networks and are supported by AI-driven autonomous navigation solutions. AI helps them to improve own capabilities in defence: more reliable real-time situational awareness, faster threat detection, better coordination of autonomous systems, optimised logistics and resource management, higher precision in target identification, reduced human deployment and exposure as well as improved battle damage assessment.[6] Unmanned military robots are able to operate effectively in high-risk and hostile environments without human exposure to danger. Without knowing and understanding the essence of military robots we are not able to analyse and assess future combat trends and security issues. So, there are some important thoughts about the nature of defence-related robotics.

Advanced military robots play special roles: they support intelligence, surveillance and reconnaissance (ISR) missions, assist combat units and enhance logistics operations. There are several types of such robots according to their area of application: ground-, air- and sea-based systems. Ground-based platforms are popular types of military robots in land warfare. These systems, commonly referred to as unmanned ground vehicles (UGVs), which operate in different terrains such as urban environments, deserts and mountainous regions. Their primary mission is to support troops with reconnaissance, threat detection and hazardous task execution. Explosive ordnance disposal (EOD) robots (see Image 2) are equipped with cameras, thermal sensors and robotic arms enabling remote neutralisation of explosive threats without direct human involvement. Aerial platforms represent probably the most known types of military robots due to their roles in surveillance and precision

[6] Artificial Intelligence (AI) in Defence; https://defence-industry-space.ec.europa.eu/system/files/2025-12/Factsheet%20AI%20in%20Defence.pdf Downloaded: 19. April 2026

strikes. Unmanned aerial vehicles (UAVs), commonly known as drones, operate without onboard crew and can be controlled remotely or run autonomously. Nowadays these platforms are indispensable in ISTAR[7] operations, during which the enemies' activity can be monitored in a large geographic area. Others can execute targeted, high precision combat operations with high accuracy. Naval operations need also robotic systems in order to strengthen maritime security and underwater situational awareness. The two different types of such robots are the unmanned surface vehicles (USVs) and the autonomous underwater vehicles (AUVs). They are used for mine countermeasures, coastal patrol, seabed mapping and submarine detection.

Image 2: L3Harris Technologies T7 explosive ordnance disposal (EOD) robot; Mike Ball: Explosive Ordnance Disposal UGVs Delivered to UK MOD; 06 Jul 2021; https://www.unmannedsystems-technology.com/2021/07/explosive-ordnance-disposal-ugvs-delivered-to-uk-mod/ Downloaded: 18. April 2026

Unmanned Aircraft Systems (UASs) are mainly used for observation (ISR), target acquisition (directing artillery fire) and also for directly attacking targets. Armed drones are usually equipped with weapons and warheads as payloads. The first is an UCAS (where the letter C stands for combat) that is fitted with hard-points for laser homing rockets or missiles and electro-optics, including a targeting laser-designator. The second is the loitering munition (LM) that can circle above the target and strike it on the command of the operator in FPV mode or automatically with detecting, tracking and identifying the adversary and later guiding the so-called kamikaze UAV with TV camera or thermal detector (heat sensor) on target. UCASs and LMs are able to attack armoured vehicles in forward positions and destroy air defence systems with more or less success depending on the enemy's counter-meas-

[7] ISTAR: Intelligence, Surveillance, Target Acquisition and Reconnaissance.

ures.[8] A drone's mission control platform (MCP) usually integrates real-time situational awareness, automated threat detection and advanced mission planning into a single, unified system. FPV drones are smart systems that use mountable AI module with spherical cameras and built-in edge analytics. This upgrade enables the UAV to process and analyse video in real time, eliminating the need to stream all row data back to the ground station that increases the chance of survivability of the drone due to its lower electromagnetic signature or emission footprint.

Counter-Unmanned Aircraft Systems (C-UAS) are technologies designed to detect, track, identify and neutralise unauthorised or malicious drones. These UAVs can threaten security in a variety of ways, including surveillance, airspace obstruction, unauthorized media and destructive payloads. C-UASs provide airspace security from these threats for critical infrastructures and VIPs. They employ a layered approach, using active and passive radars[9], radio frequency (RF) sensors, EO/IR (electro-optical and infrared) cameras and acoustic sensors to detect, track and classify drones in real-time. For mitigation and neutralisation of drone activities soft-kill (communication disruption between the drone and pilot by jamming and spoofing) or hard-kill (physical destruction or capture with nets, high-energy lasers, kinetic projectiles, interceptor missiles and drones) measures that might be especially successful. The multi-sensor fusion (or simply sensor fusion) helps to make C-UAS methods more and more effective. C-UAS technologies might be fixed-site systems (permanently installed around sensitive areas like airports, power plants or other critical infrastructure), portable/backpack solutions (mobile, rapidly deployable systems for troops or temporary event security) and AI-driven systems (AI is increasingly used to reduce false positives, birds vs. drones). Key advantages of using radar systems in drone include: long-range detection (identifying drones at greater distances compared to optical or acoustic sensors, providing early warning and extended response time), all-weather performance (effective operation in diverse environmental conditions, including darkness, fog, rain and other weather scenarios where visual or acoustic sensors may be compromised), simultaneous tracking (monitoring multiple drone targets simultaneously, effectively managing drone swarm scenarios and complex airspace environments) and detection of RF-silent drones (without emitting radio frequency signals they are undetectable by RF-based sensors). [10] Based on integrated data from multiple external sensors, AI-driven pattern recognition algorithms identify and predict threats. These early warnings give operators more time to respond that is their best advantage.

[8] Stephen W Miller: Countering Tactical UAS and Loitering Munitions; Military Technology Vol. XLVI 3/2022; ISSN 0722-3226 p 26–31

[9] The active radar transmits signals actively and analyses reflected signals, providing precise target detection and tracking. The passive radar does not emit signals but instead detects and analyses reflections from external signals, such as broadcast or communication signals. This makes passive radar inherently stealthy, as it does not emit detectable signals itself, making it suitable for sensitive or covert operations.

[10] The Comprehensive Guide to Counter-UAS; https://www.dedrone.com/white-papers/counter-uas Downloaded: 9. April 2026

Remotely guided and autonomous ground weapons systems, missiles, canons and machine guns are especially dangerous. Automatic ground ISR platforms (often built on UGVs) are able to provide real-time intelligence on the enemy in form of video streams, voices and multispectral images in a map. Autonomous weapons systems now operate mainly under human supervision in order to maintain the balance between operational efficiency and to comply with international humanitarian law. Unmanned logistics vehicles are responsible for supporting military operations by ammunition, food, fuel, medical supplies and casualty evacuation. In a modern military operation these UGVs are contributing to the success of the mission and the resilience of the troops. Their possible kinetic effectors can increase human firepower and stand-off capabilities. AI-supported UGVs move autonomously and they enhance tactics like force multipliers and have solutions for avoiding casualties and also will have similar capabilities as their air mates in the near future.[11]

Programmable ammunitions are advanced weaponry with electronic fuses that can be set to detonate at a specific point in the air (airburst), usually at an effective distance from a target. These rounds increase lethality against drones and hidden targets with optimising fragment distribution. Having a powerful precision projectile is an important aspect of an effective military attack. With the advancement of smaller electronics, more sophisticated and highly controlled detonations have become possible. For example, while a direct hit against enemy ground forces can wreak havoc, airbursts or detonation in air above the target can be even more efficient, as it allows for a wider area of coverage. One of the many examples is the Rheinmetall's AHEAD[12] programmable ammunition, which is designed for defence against approaching enemy weapons. Fired from a 35 mm cannon and paired with the Skynex system[13], each round is immune to electronic countermeasures and can engage quick aerial threats by calculating when to intercept and activate its fuse accurately.[14]

Military robotics is more and more present among various tools of modern warfare strategies. Their task is to improve operational efficiency, to enhance battlefield awareness and to reduce risks to human beings. Emerging technologies like swarm robotics, enhanced autonomy and smooth human-machine collaboration are featuring modern warfare. These unmanned and autonomous systems reshape current military conflicts and wars. Precision, speed and data-driven decision are the main attributes of a modern combat moving towards the robotic warfare.[15]

---

[11] Marco Giulio Barone: The Continuing Evolutions of UGVs – Interview with Milrem Robotics; Military Technology Vol. XLVI Issue 3 2022, ISSN 0722-3226; p 76–77

[12] ALWAYSAHEAD – OERLIKON AHEAD AIR BURST AMMUNITION; https://www.rheinmetall.com/Rheinmetall%20Group/brochure-download/Weapon-Ammmunition/B038e0424-Oerlikon-Ahead-Air-Burst-ammunition.pdf Downloaded: 19. April 2026

[13] Networked air defence – Oerlikon Skynex air defence system; https://www.rheinmetall.com/en/products/air-defence-systems/networked-air-defence-skynex Downloaded: 19. April 2026

[14] Shane Schmid: What are programmable munitions and what advantages do they give to the military? https://www.slashgear.com/1925422/programmable-munitions-explained-how-benefit-military-advantages/ Downloaded: 7. April 2026

[15] Types of Military Robots: An In-Depth Analysis of Modern Robotic Warfare; https://www.kingsresearch.com/blog/are-military-robots-redefining-laws-of-war Downloaded: 31. March 2026

Image 3: Skynex air defence system produced by Rheinmetall. Heavenly forces for Italy; https://spartanat.com/en/heavenly-forces-for-italy Downloaded: 18. April 2026

Main disruptive technology measures and procedures of the robotic warfare

Disruptive technologies and procedures leave or put aside old techniques and measures and provide a brand-new solution, which is much more effective, resilient or sustainable than the earlier one. The robotic warfare would like to use these disruptive tools and methods in order to be better than its conventional predecessor. In the following there are listed some measures and procedures as asymmetric warfare, swarm intelligence (SI) and swarm drone system, cloud computing, Anti-Access / Area Denial (A2/AD) tactics, artificial intelligence (AI) and IT warfare that disrupt with old traditions and provide new benefits. We will see that drones usually play a central role in robotic procedures.

Asymmetric warfare means that a significantly weaker belligerent party uses unconventional strategies, tactics and methods against the stronger party in order to mitigate own conventional inferiority. Examples of asymmetric warfare include guerrilla warfare, terrorist tactics and a war between a country that is able to use nuclear weapons and one that is not. Throughout history, asymmetric tactics have been valuable first of all in guerrilla warfare, where fighters, usually fewer in number and with less powerful weapons, have used tactics such as ambushes and cutting communication lines to erode the enemy's will to sustain the costs of war.[16] Asymmetric warfare is a strategic choice forced by a wide structural gap in defence spending and technology. It allows the weaker party to avoid a predictable defeat in a conventional conflict and instead create a prolonged, unpredictable and costly conflict. Techniques include terrorism, cyber sabotage and drone warfare that are to target vulnerabilities rather than matching strength. Generally, the stronger party is not able to use all its capacity but the weaker one is able to employ all its limited tactics and tools. Methods are designed to cause disproportionate damage and raise the cost of conflict for the stronger party, often targeting communication lines and

[16] Asymmetrical warfare; https://www.britannica.com/topic/guerrilla-warfare/Origins-of-modern-guerrilla-warfare Downloaded: 4. April 2026

economic assets directly or indirectly with eroding the public morale. Modern examples include using low-cost military drones for surveillance or kamikaze attacks against expensive precision weapons, as well as utilizing proxies to avoid direct confrontation. Iran has been using a relatively cheap drone technology and missiles to threaten conventionally superior forces like the United States and Israel. Combatants often operate within civilian populations, making it difficult for the stronger force to target them without causing collateral damages. Ukraine also often applies consumer drones and distributed small robotic units to hold off the larger Russian invasion force.

Swarm intelligence (SI) is based on natural examples and defined as a method using AI and inspired by the collective behaviour of social insects or animals. It is utilised in the design of intelligent multi-agent systems to achieve complex goals through collaboration. It involves decentralized, self-organized systems – often land robots or aerial drones – modelled after natural behaviours of bird flocks, school of fish, swarm of bees or ant colonies. These systems enable multiple agents to cooperate on complex tasks, enhancing efficiency in defence, search-and-rescue and logistical operations through collective decision-making and real-time data sharing. No centralised control mechanism dictates the rules of individual agents, instead, they act locally according to an intelligent global behaviour with a certain degree of randomness and instinct.[17] Swarm technology in defence involves multiple autonomous, AI-enabled unmanned systems (for example ground vehicles, aerial drones and vessels) collaborating with each other. Key features include intelligence gathering, overload attacks and electronic warfare (EW) to overwhelm defence, offering high adaptability and cost-effectiveness. These systems operate with limited human oversight, enabling rapid machine response to different threats. Swarming is slowly becoming one of the most significant advancements in autonomous defence systems. As modern forces face faster, more complex and more distributed threats, swarming technology represents the next major evolution in military capability. Swarm operates as a collective intelligence and its main advantages are: scale and saturation (overwhelming traditional defence), resilience, speed and adaptability.[18]

A swarm drone system is a networked group of small autonomous UAVs that work together as one unit. Each drone communicates with the others, sharing data in real time and adjusting its actions based on the group's overall mission. Rather than depending on a single large drone, the workload is spread across dozens, sometimes hundreds of smaller units. This collective approach makes the system incredibly resilient. If one drone is damaged or lost, the rests instantly adapt and continue the mission without disruption. This flexibility and built-in redundancy give swarm drones a major advantage in complex or hostile environments where reliability is

[17] Swarm Intelligence – In subject area: Engineering; https://www.sciencedirect.com/topics/engineering/swarm-intelligence Downloaded: 7. April 2026

[18] Swarming in Defense: How Autonomous Systems Transform Modern Operations; https://orbotix.tech/swarming-in-defense/ Downloaded: 19. April 2026

critical. Mission control platforms are moving from the ground to the air due to advanced technologies. The military use of swarm drones might be: surveillance and reconnaissance (providing real-time territory monitoring and imagery), target identification and tracking (observing targets from different angles), EW and deception (overwhelming radar systems, creating false signatures and acting as decoys), precision strikes (on enemy positions, radar stations, vehicle convoys or communication nodes), sensor deployment (dropping seismic, acoustic, thermal or chemical sensors across immense terrain), search and rescue operations (scanning large areas simultaneously to locate survivors and guide rescue teams), communication relay (airborne network that restores communications in areas where signals are jammed or infrastructure is destroyed), terrain mapping and route planning (updated maps of unfamiliar or hostile environments), urban warfare support (in dense cities gathering intel and delivering small payloads), border and territorial security (monitoring borders, coastal areas, bases and checkpoints). Furthermore, swarm drones can provide last-mile resupply (delivering ammunition, food, water, batteries, fuel and medical packages directly to troops under fire, bridging the most dangerous last mile in military logistics), medical support (carrying blood, first-aid kits and medicines to injured soldiers) and rapid support delivery in contested zones (navigating around blocked roads, destroyed bridges and hostile terrain). The swarm drones' flexibility, resilience and cost-efficiency make it possible to take part in missions that were once too risky, too slow or too resource-heavy for traditional forces.[19] We can state that swarm drones (see Image 4) have quickly become vital part of the modern battlefield thanks to their widespread operational advantages.

Image 4: A swarm of drones at Fort Irwin, Calif., in 2019; Jennifer H. Swan: Air Force aims to gauge industry interest in making atomic clock to guide drone swarms; September 8, 2025; https://www.stripes.com/branches/air_force/2025-09-08/air-force-exploring-drone-swarm-capabilities-19018645.html Downloaded: 18. April 2026

[19] Swarm Drones: Applications, Benefits, and Real-World Use Cases; https://bonvaero.com/swarm-drones-applications/ Downloaded: 7. April 2026

Cloud computing is an especially smart solution in case of limited capacity of storing and processing big data on the scene. In every domain, the importance of data is immense. Organisations and individuals often use physical devices such as hard drives to store data, but it has a limited capacity that may delay several processes. This method makes it easy for large-scale organisations to store their data in a cloud, upload their files and access them anytime. Recently defence establishments also use cloud computing and private sector services. This system can provide decisive information to soldiers during operations since communication and information transfer are crucial on the battlefield. As a result, this system could provide better operational capabilities. Nations and their armed forces today want to leverage the potential of AI for intelligence gathering and other military purposes. Cloud storage might be used by military establishments to secure their information and later download it to train their AI model or analyse past performance. The AI model, based on the information fed, can create strategies, suggest improvements and identify or predict future threats.[20]

Anti-Access/Area Denial (A2/AD) tactics are military approaches designed to prevent an adversary from entering an operational area (Anti-Access) and restrict its freedom of action within that territory (Area Denial). These methods use layered, long-range and precision-guided systems – such as advanced missiles, air defences and cyber tools – to force adversaries into costly, high-risk or slow-paced actions. Military strategists frequently use the term A2/AD to refer to war-fighting strategies aimed at preventing an adversary from deploying military forces in close proximity to, inside of, or within a contested area. The strategy makes possible to use a number of interconnected missiles, sensors, guidance and other technologies to restrict mobility in order to deter any potential adversaries. Anti-ship, anti-tank, layered coastal defence, layered air defence and integrated air and missile defence are some examples of A2/AD.[21] As the most powerful military alliance also NATO and its member states should deal with A2/AD challenges and look at weaponry and weapons systems that would be used in denying access. Equally important is a comprehensive analysis of NATO-members' capabilities to maintain a strategic and technological edge, so as to guarantee this access, whenever and wherever it might be needed. A2/AD can be seen as a policy challenge that requires NATO to fully understand what is at stake and how it can properly respond, while taking into account the risk of a possible escalation.[22] One of the imminent operations conducted

[20] Jatin Chawla: Cloud Computing in the Military; https://www.thegeostrata.com/post/cloud-computing-in-military Downloaded: 7. April 2026

[21] What is Anti-Access Area Denial Strategy; https://defensetalks.com/what-is-anti-access-area-denial-strategy/ Downloaded: 7. April 2026

[22] How to Respond to Anti-Access/Area Denial (A2/AD)? Towards a NATO Counter-A2/AD Strategy; https://www.ndc.nato.int/fr/new-research-division-publication-how-to-respond-to-anti-access-area-denial-a2-ad-towards-a-nato-counter-a2-ad-strategy/ Downloaded: 7. April 2026

with the A2/AD tactics was the Iranian military closing of the Strait of Hormuz on the 4th of March 2026 to the American and Israeli ships that had been successful for a while.

Artificial intelligence (AI) is a technology that enables computers and machines to simulate human learning, comprehension, problem solving, decision making, creativity and autonomy. Applications and devices equipped with AI can see and identify objects, understand and respond to human language, learn from new information and experience, make detailed recommendations to users and experts. These can act independently, replacing the need for human intelligence or intervention. Key aspects of AI are machine learning (ML – algorithms that improve their performance over time by analysing data rather than being explicitly programmed for every task), deep learning (DL – a subset of ML that uses neural networks with many layers to analyse complex patterns), generative AI (Gen AI – that creates new content, such as text, images or music, based on learned data patterns) and natural language processing (NLP – the capability of machines to understand and interpret human language). In 2024, most AI researchers, practitioners and AI-related headlines were focused on breakthroughs in Gen AI, that can create new content. AI is rapidly evolving from simple rule-based systems to sophisticated, generative models that are actively transforming the modern digital landscape. AI offers numerous benefits across various industries and applications. Some of the most commonly cited benefits include: automation of repetitive tasks, more and faster insight from data, enhanced decision-making, fewer human errors, 24x7 availability and reduced physical risks that are especially important in military operations as well.[23] There is a broad acceptance within military circles that AI will make its way onto the battlefield in the foreseeable future. But it is not decided yet what role it should be allowed to take. Beside several forms of decision-making support in targeting, AI is able to help politicians and governments with defence related conflict forecasting, escalation scenarios and crisis responses in order to save lives before it becomes too late.[24]

Information, electronic and cyber operations seem to exist separately and independently from each other but the truth is that they are very well interconnected. Information operation focuses on the message and content, EW mainly deals with hardware (newly also with software defined radios – SDR) and signals (like frequency hopping – FH), while cyber activity (attacks and protection) primarily refers to software and data. Now they are in close contact with each other and their common platform is the information technology (IT). So, I would recommend a new expression, the IT warfare that can cover all the three forms related to a complex combat procedure. Nowadays ground, air and maritime hegemony is not enough to win a battle separately, all domains should be connected with each other in one

[23] Cole Stryker, Eda Kavlakoglu: What is AI? https://www.ibm.com/think/topics/artificial-intelligence Downloaded: 10. April 2026

[24] Samuel Cranny-Evans: The Role of AI in Warfare; Military Technology Vol. XLVI Issue 1 2022, ISSN 0722-3226; p 56–57

or more internet of things (IoTs). A dominant belligerent should own or influence also the adversary party's motivation and will with the help of IT warfare. This is undeniable that communication is one of the most important parts of a military operation. Without a safe datalink network, missions are useless and obsolete. Due to security reasons navigation (Global Navigation Satellite System – GNSS) and communication platforms move to the sky (space) so observation and communication satellites provide flawless image flow or datalink and Elon Musk's Starlink satellite constellation delivers broadband internet access to the Earth.[25]

Analysing the military robots and autonomous weapons as well as disruptive technology procedures I created an illustration on the hypothetical and schematic structure of a possible multi-domain robotic warfare that is shown in the Figure 1. Shortly explaining the picture, the human factor is connected to the machines with human-machine interface (HMI) and they work together in a so-called manned-unmanned teaming (MUM-T) model. Machines supported by AI conduct special robotic tasks, measures and procedures while communication provides the connection, navigation and information access in a network inside and with other independent systems.

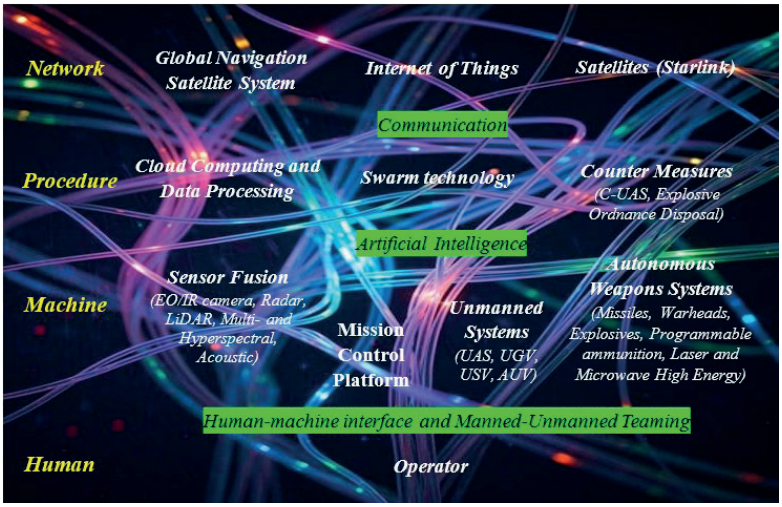

Figure 1: Schematic structure of the multi-domain robotic warfare; The author's own illustration; Created: 17. April 2026

Preconditions for waging a possible robotic warfare

After getting to know some basic information of the robotic warfare we can state that now only great powers are able to prepare and wage a limited scale of the most modern warfare since it is especially expensive and resource intensive. Human capabilities should be available all the time of the preparation phase and during the

[25] Satellite Technology; https://starlink.com/technology Downloaded: 10. April 2026

operation as well. It means also that weapons and materials should be supplied long-term and continuously, otherwise operations will not be successful.

In my opinion the well-known PESTEL analysis (see Figure 2) might help us to understand the basic requirements of the robotic warfare. PESTEL means political, economic, social, technological, environmental and legal assessment of a problem or a phenomenon. This method is a strategic framework used to analyse the external macro-environmental factors. It helps identify risks and opportunities to form a strategy, create a risk management and make related decisions. PESTEL exactly deepens the understanding of the external environment and examines broader societal and global trends.[26] Let's see the six components one by one in relationship with robotic warfare and later on one extra that is not part of PESTEL.

Figure 2: Categories of PESTEL analysis. What is PESTEL Analysis? https://www.lumovest.com/library/management-strategy/pestel-analysis/ Downloaded: 18. April 2026

Robotic warfare capabilities need a widespread political consensus in a democratic state. Non-democratic countries are able to make decisions (among others also military one) easier and faster but they have only limited capabilities to build up modern and well-equipped armed forces that is able to conduct robotic warfare. In a certain democracy parliament makes laws and regulations and government fulfils them. The national security, defence and military strategies of a country punctually define the potential warfare concept that suits to the military opportunities and security threats of a state. Political agreement is inevitable in order to establish the organisational frame and provide required resources (human and material) of a robotic warfare. Defence policy of a state depends on the geopolitical environment and the future trends. These aspects should be taken into consideration during the preparation for a robotic warfare establishment that needs a proper organisation, infrastructure, staff, military technology and budget. Politics should prepare for conflicts and wars, since after Clausewitz, war is the continuation of politics with other means.

A reliable and stable economic background of a country is a precondition for maintaining modern armed forces and their possible robotic warfare capacity and

[26] PESTEL Analysis: What It Is and How to Use It for Strategic Planning; https://www.spiderstrategies.com/blog/pestel-analysis/ Downloaded: 7. April 2026

capability. Besides the continuous decent economic growth, a prudent fiscal and financial policy is also important in order to avoid imbalances among different sectors as healthcare, education, public administration, internal and foreign affairs, law enforcement, environment, culture, security, defence and so on. A strong economy provides financial resources and manufacturing capacities for procurement and production of cutting-edge military technologies. The own defence industry mitigates foreign dependency and increases the resilience of the country. Nowadays the access to conventional and renewable energy resources and to the so important raw materials plays also an enormous role. Only some great powers (US, China and Russia) are able to cover own demands from their own resources. Since robotic warfare is resource-intensive only great powers are ready to establish the base for this modern fighting style. The economy determines the form of warfare, but warfare affects the economy as well. From disrupted exports to military spending, the economic consequences of a war extend far beyond the battlefield. The ongoing conflicts in Ukraine and the Middle East have devastated civilian life and regional economies alike. In either case, the economic damage leaves challenges for governments, industries and citizens since it is not just infrastructure that needs to be rebuilt, but entire social life.[27]

Social factor is not less important than politics and economy. A country's society provides the human factor and resource for the defence and military capabilities. Cultural heritage, religion and national traditions play also a huge role in creating modern armed forces. Demographic processes and so the youth is crucial in this sense since the future is represented by young people who are able to handle new IT technology, which is becoming more and more dominant in the military arsenal. Public opinion is also really important in defining the military strategy and deciding about war and peace. A modern society is usually against wars and armed conflicts but if these are inevitable average people expect and accept only limited human losses, casualties and material damages. A robotic warfare needs high-educated experts and soldiers who are well-trained and physically and psychologically chargeable.

It is worth speaking about, but it is not needed to prove that technological factors drive innovation and strengthen competitiveness in a country. A nation should have a high level scientific and technology development level in order to give the right answers to several security and military challenges. Modern warfare is technology-driven and this is the reason why military capabilities are measured by technological development, engineering capability and production capacity. Digital transformation trends, including automation, AI and connectivity offer operational efficiency opportunities while they simultaneously challenge traditional models.

[27] Mia Fried: Economics of Warfare; https://sites.lsa.umich.edu/mje/2025/05/22/economics-of-warfare/ Downloaded: 19. April 2026

Technological change (as the additive 3D printing, digital design, Industry 4.0[28] and others) shortens development and production lifecycles. New cutting-edge military technology needs new counter-products and -measures on the other side of the belligerent parties. Robotic warfare now looks much more a technological qualitative race than a quantitative human and material competition among adversary states that has been a long general phenomenon. It is not true that nowadays the number of warheads, missiles, tanks, armoured personal carriers, fighter jets, helicopters and drones are not important. Old and new military technology should exist in parallel and smartly in order to be able to react to multi-domain threats of conventional and robotic warfare properly.

Climate change impacts increasingly force also defence ministries and armed forces to reassess their strategies, operations, supply chains and resource dependencies. Rising sustainability expectations from the military push strategists and leaders of the defence industry toward environmentally conscious practices, creating both compliance to environmental requirements and military effectiveness. Sustainability is appearing more and more important in the armed forces on the level of military technology, operations and structure as well. Environmental factors are slowly evolving from peripheral concerns to central strategic considerations in the military. Robotic warfare might support the environmental-friendly endeavour with its resource-conscious operations but it should be controlled continuously, otherwise sustainability will be sacrificed for the military success. Climate change presents a systemic challenge to society that is driving an unprecedented sustainable technology revolution. Participating in this revolution has the opportunity to improve the agility, resilience and capability of the armed forces as well. The potential impacts of climate change on current and future operating scenarios are increasingly understood, as is the general transition away from fossil fuels (decarbonisation) and increasing the volumes of sustainable aviation fuel (SAF). Both factors require the defence sector to think about climate change adaptation and its implications for products and capability and the requirement for energy resilience and security both in platforms and across infrastructure and bases. Sustainable technologies have potential to support and enable the sustainment and efficiency of military operations. Therefore, there is a need for defence to better understand where adapting can offer financial rewards, or prevent financial losses.[29]

[28] Francesco Tucci: Implications of the Industry 4.0 Concept On The Defence Sector; Military Technology Vol. XLVIII 1/2024; ISSN 0722-3226 p 37–39

[29] Defence: sustainability as a competitive advantage; 11 October 2024; https://www.gov.uk/government/publications/defence-sustainability-as-a-competitive-advantage/defence-sustainability-as-a-competitive-advantage Downloaded: 19. April 2026

International and national legal actors establish the regulatory framework for the defence industry and military conflicts or wars. Especially dual-use products regulations and anti-proliferation weapon restrictions and bans might create a visible and transparent picture on arms trafficking and proliferation. Illegal weapon transfer might cause surprises and serious threats to regular military and legal security forces. Without clear legal frameworks, standards, rules and sanctions the international stability and security might easily become fragile. Not only for conventional operations but for the robotic warfare new international regulations are needed in order to avoid machine- or AI-decisions causing unacceptable and disproportional damages and losses, possible civil casualties. Law is usually falling behind technological development and this is the reason why new technologies might be used for still legal but unethical goals. New disruptive technologies easily can cause huge intentional and unintentional damages if they were applied not lawfully.

Interdependency of the above mentioned six factors is a fact that should be taken into consideration. Among material preconditions and background, political will is also important to build up up-to-date capabilities and preconditions of the robotic warfare.

Since PESTEL analysis does not have a military part, I would like to enhance it with some interesting defence-related statements and assessments. Military operations nowadays do not reach a full-scale war since it has no sense. The most common combat level is maximum the battalion battlegroup mission but brigade, division or corps do not fight long-term because of their costs, damages and casualties. Expeditionary forces usually hope that they can conduct a short-term and devastating strike against the enemy or fight long-term with low intensity. We might think that military robots and autonomous weapons are able to substitute soldiers but these machines are especially supply-intensive. Even a semi-robotic warfare consumes a plenty of missiles, drones, ammunitions and payloads. Not only small countries but also great powers do not have enough reserve parts and consumables for their military operations, however, these are inevitable for keeping the enemy far from the own troops and infrastructure. Old military values and capabilities, as for example defence and protection (nowadays resilience), mobility and firepower are even today very important in the age of AI, digitalisation and software. New technologies like drones change operation planning that awaits an adaptable combat control and different decision-making. Brand-new military procedures and operational measures are not able to be completed due to the high intensity of fights, the time-shortage and the always changing conditions. Usually, the doctrine and strategy are not up-to-date either, because of similar and different reasons. The least one is a huge political concern since consensus on a common strategy is usually missing in a multi-party parliament or in a diversified alliance. It is unambiguous that military robotics is at the centre of modern warfare strategies, which aims the improvement of operational efficiency, enhancement of battlefield awareness and

Image 5: Stryker combat vehicle equipped with short-range air defence weapons (General Dynamics Land Systems) Army Inks $1.2 Billion Deal to Equip Strykers with Short-Range Air Defense Weapons; October 02, 2020; https://www.military.com/daily-news/2020/10/02/army-inks-12-billion-deal-equip-strykers-short-range-air-defense-weapons.html Downloaded: 19. April 2026

reducing risks to civil and military personnel. However, the controversy remains, the enhanced efficiency often causes growing threats of uncontrolled activities.

Misconceptions, miscalculations and overestimations of the robotic warfare

Idealists might think that the robotic form of warfare will be much more comfortable for mankind since there will be no or less human losses thanks to the up-to-date precision weapons and AI, but this is not true. Unfortunately, the essence of the war is always the human factor. People decide about the war, they wage it with military technology and they stop it after losing its sense. In many cases only huge damages and casualties (human losses) are able to put an end to wars. It might mean that also a robotic warfare will reach its aim only after significant human, sometimes civilian losses. To be frank, nobody cares about losing tanks, artilleries, fighter jets and missiles if there are no human casualties. However, the civil society is against obsolete hardships, sufferings and deaths so it can influence the outcome of wars as well.

A big country that probably can afford waging an expensive robotic warfare might think that everything is reachable. It can start a military air strike or ground operation with modern military power against a less developed adversary. The stronger belligerent might assess that a lightning operation is enough to defeat the enemy. Usually, this country does not calculate with asymmetric warfare that is often seems to be effective against the dominant foe. Asymmetric warfare is able to slow down the dynamic of an armed conflict and sometimes to stop the advancement of the aggressor. Robotic warfare is not omnipotent and it needs an equal opponent. This is a big controversy that questions the raison d'etre of robotic warfare as well.

Many think that the robotic warfare seems to be mainly a machine-led solution where human beings are not exposed to direct violence, so in this sense they are not so important. However, human operators and commanders will be further important in leading military operations. Only a (low level) part of decision-making and detection activity should be handed over to robots in order to enhance or substitute limited human capacities and capabilities (especially perceptions). Machines will support politicians and soldiers with their robotic features in crucial situations. The role of human being is not disappearing but amending in a theoretical robotic warfare, since it has a plenty of psychological and reality reasons. Empirical experiences consistently reaffirm the decisive role of human personnel, mainly technical competence, cognitive adaptability, leadership and morale even in a modern warfare. As a result, technologies are judged too fragile, costly or easily disrupted to deliver decisive advantages. Conventional fires, traditional military mass and resilient human factors partially regain primacy. Furthermore, in many contemporary cases, technology has primarily enhanced human performance rather than replaced it.[30]

Remotely guided robots and autonomous weapons face several "deadly" challenges. Their operators do not risk their own lives so sometimes they do not care about the loss or recovery of these machines. Remote pilots occasionally undertake risky operations (in bad weather conditions, during an opportunity of losing control due to the unknown terrain or electronic interference, jamming) that can lead to the loss of expensive precision weapons and cutting-edge military technology. Limited energy (battery or fuel) capacity of a robot is another risk. The timely wrong-planned operation might lead also to early battery discharge or running out of fuel. Individual robots might operate alone without any physical or electromagnetic support that makes them vulnerable to adversary counter-measures. In this case groups or swarms of these guided or autonomous robots and weapons are more resilient of electromagnetic (participants communicate with each other instead of the ground station) or kinetic (one loss or some losses do not mean the end of the operation) counter-attacks in the sense of the success of their operation. Robotic warfare needs a special infrastructure and supply chain that are not affordable for every military.

While swarm drones offer enormous potential, they also face several tactical and logistical difficulties that limit their full-scale use on the battlefield. They also have limited endurance and range since short battery life restricts how far and how long swarms can operate, affecting both supply missions and long-duration surveillance tasks. Individually, these drones can only carry small loads because of their payload limitations. Managing the movement and decision-making of dozens or hundreds of drones requires advanced AI and complex coordination. Any failure in communication or algorithms can disrupt the formation and mission. Due to vulnerability to EW, jamming, GPS spoofing and cyberattacks can break the

[30] Ivan Zaccagnini: Emerging Technologies and the Enduring Elements of Warfare; STRATEGIC TRENDS 2026 – Key Developments in Global Affairs; Center for Security Studies; https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/ST2026-C3-IZ.pdf Downloaded: 19. April 2026

unintelligent swarm's communication link, confuse simple navigation systems, or cause conventional drones to scatter or fail. Strong winds, rain, snow, heat or dust (weather sensitivity) can significantly impact lightweight drones, reducing mission reliability during harsh conditions. Although swarms are not easy to target and hit, large numbers of drones still generate noise and electronic signatures that can be picked up by advanced enemy sensors, so the risk of detection is high in contested environments. Deploying and sustaining hundreds of drones demands continuous charging, storage, repairs and coordination creating a new layer of logistical complexity that causes maintenance and operational burden. Using multiple drones in congested or dynamic war zones requires strict control to avoid interference with friendly aircraft and ongoing operations that raises airspace management issues. Until these tactical and logistical challenges are not solved, swarm drones will remain powerful support assets enhancing military logistics and operations, but not fully replacing conventional systems.[31]

Security challenges of the robotic warfare

Robotic warfare is extremely dynamic in terms of its varied operations. Without a comprehensive and complex preparation and planning it does not work properly. Unfortunately, also own military robots might cause boomerang effects and friendly fire if they are not appropriately programmed or guided. The other challenge might be the violating international rules with causing disproportional collateral damages and war crime. Humanitarian catastrophe must always be avoided.

Autonomous weapons systems are often referred to killer robots that use sensor processing and AI to independently identify, select and engage targets without human intervention. These systems can make lethal decisions on their own that certainly might raise ethical, legal and security concerns. Some autonomous weapons systems have existed for many years but the types, duration of operation, geographical scope and environment in which such systems operate have been limited. Now technological advances are stimulating the development of these killer robots, which would operate without meaningful human control, delegating life-and-death decisions to machines. The UN and other international bodies are in ongoing discussions about how to define and regulate (or potentially ban) lethal autonomous weapon systems (LAWS), emphasising the need for continued human control over the use of force. Human Rights Watch is a founding member of Stop Killer Robots campaign, a civil society coalition that calls for a new international treaty to prohibit and restrict autonomous weapons systems.[32]

[31] Swarm Drones: Applications, Benefits, and Real-World Use Cases; https://bonvaero.com/swarm-drones-applications/ Downloaded: 7. April 2026

[32] Killer Robots (Human Watch Rights); https://www.hrw.org/topic/arms/killer-robots Downloaded: 3. April 2026

Whereas in many cases of unmanned military drones the decision to take a life is made remotely by a human operator (as it is usual in the case of the MQ–9 Reaper, see the Image 8), with autonomous weapons the decision is made by algorithms alone. An autonomous weapons system is pre-programmed to kill a specific target profile. Weapons that use algorithms to devastate and are not controlled by human judgement are immoral and pose a serious threat to national and global security. The United Nations Secretary General António Guterres argues that "machines with the power and discretion to take lives without human involvement are politically unacceptable, morally repugnant and should be prohibited by international law." Delegating the decision to use lethal force to algorithms raises significant questions about who is ultimately responsible and accountable for the use of force by autonomous weapons.[33]

Image 6: MQ–9 Reaper medium-altitude long-endurance (MALE) remotely piloted aircraft; Zamzam Channa: Lethal Autonomous Weapon Systems: A Gamechanger Demanding Regulation; March 26, 2024; https://www.geopoliticalmonitor.com/lethal-autonomous-weapon-systems-a-gamechanger-demanding-regulation/ Downloaded: 18. April 2026

While AI increases productivity and offers new avenues for innovation, it also presents challenges as for example ethical concerns (bias, data privacy and transparency in decision-making), economic impact (potential job displacement due to automation) and resource intensity (high environmental costs related to energy and water consumption in large-scale computing).[34] AI is the most energy consuming solution that is affordable only for great powers. The other problem is that these strong states (as the United States[35]) do not want to talk about the exclusively peaceful use of AI since they want to protect their interests and rights to defend themselves with any tools and means supported by AI applications. In my opinion, we

[33] Autonomous Weapons; Slaughterbots are here. The era in which algorithms decide who lives and who dies is upon us. We must act now to prohibit and regulate these weapons. https://autonomousweapons.org/ Downloaded: 3. April 2026

[34] Cole Stryker, Eda Kavlakoglu: What is AI? https://www.ibm.com/think/topics/artificial-intelligence Downloaded: 10. April 2026

[35] Ensuring a national policy framework for artificial intelligence; Executive Orders; December 11, 2025; https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/ Downloaded: 10. April 2026

firstly do not have to be scared of AI's hegemony over humans but the humans who use the AI for their hegemony. Besides, we have to take into account as well that AI is going to have a special impact on the society, the education, work and human-machine connectivity which is controversial since AI is also a dual-use invention.

Military and intelligence services around the world cooperate with private companies. This model has worked very well in the United States, where most of the defence contracts are given to private firms. As a result, the US military gets the most advanced technology. While national security benefits from the involvement of private companies, it also poses a serious threat of espionage or information leaks. In the past, there have been successful attempts to access sensitive information about the US military through the channels of private firms. As a result, the state needs to ensure that the system is secured and that private firms have no access to military applications once they are in use. As global warfare changes, military and intelligence agencies adapt new ways to deal with threats. We live in an era where private and military partnerships are essential for the new-age warfare. On the one hand, civilians empower the military with new capabilities and promote research in the military domain, while on the other hand, they give power to private firms and big tech, by making the military dependent on such firms. Too much dependence and trust in the private sector might harm the national interest, as these firms function independently and cannot be forced to do something differently. Governments should set up a system to monitor the development and functioning of firms that are in some way involved in connections with the military and intelligence agencies.[36]

We do not have to chase illusions. A possible proliferation and illegal trade of advanced technologies is a fact. Cutting-edge military techniques easily can land in the hands of criminals and terrorists. They are interested in making chaos at their territory of operations where civilians and also soldiers might become victims of their assassinations committed by military robots and autonomous weapons. Now these new disruptive technologies are especially expensive, so they are not affordable for many organisations but usually the price is not a big burden. Mafia organisations are ready to procure killing robots from the black market for their ill-intentioned customers who pay for the service with black money originated also from criminal activities. So, one of the most crucial security challenges remains the illegal arms trafficking that is able to provide killing robots that do not risk the life of their operators, the real perpetrators, also terrorists. Beside the high price cutting-edge technology has another restraining force and it is the resource-intensity that expects human knowledge and material infrastructure as well. Unfortunately drones as dual-use disruptive technologies are an exception in many aspects. They are cheap, easy to procure and simple to operate.

[36] Jatin Chawla: Cloud Computing in the Military; https://www.thegeostrata.com/post/cloud-computing-in-military Downloaded: 7. April 2026

In summary, application of military robots is inevitably raising the question of their ethical and humanitarian impacts. Issues related to autonomous decision-making, civilian protection (avoiding collateral damages) and accountability remain central to global security discussions. Defence organisations are actively dealing with policies to ensure responsible use of autonomous weapons and its compliance with international regulations. Ethical deployment is essential for maintaining legitimacy and stability in modern warfare, so in the robotic warfare as well.

Conclusions

Nowadays we are in a labile stage between a hot peace and cold war of the international relations where great powers confront with each other and often judge about other nations' fate due to their interests. Despite the fast technological development in recent years, we should state that robotic warfare is not able to become full-scale and might not be implemented short-term. Conventional strategies and new methods do not exist long and alone since counter-measures are developing extremely fast. According to the geopolitical environmental effects and changes, strategies often should be reviewed, operations amended and tactical procedures adapted to new requirements. However, limited robotic combats led by autonomous machines and weapons might be successful.

Robotic warfare currently does not exist as a real strategy since its preconditions are still missing. Every armed conflict or war has its own peculiarity and it is made by a combination of conventional, information, electronic and cyber warfare. The military operation usually becomes also hybrid in the sense of using political impact, economic pressure, social influence and technological race in the reality or at the cyberspace. Today military conflicts are so complex and widespread in their forms that a human brain is not able to understand its complicated processes. This is the reason why strategists use AI and other disruptive solutions in order to simplify decision-making procedures and react properly to new challenges. During modern military missions the speed is crucial but human capabilities are not fast enough to respond to unexpected events in a timely manner. So, it is not a surprise that robots and machines substitute soldiers in order to act faster, more precise and much effective during a strike or defence operation. The future robotic warfare should be varied, involving conventional and modern military aspects as well. It will not be better or worth, it will be different.

This is unambiguous that human factor is the most critical point in every military operation but it is not only because of soldiers. If politicians decide about war, they try to convince their public opinion about the sense of waging it. At the beginning of the hostilities, citizens believe that military strikes and operations against the enemy will be short and not so painful but later on the endless fight is becoming harsh and unbearable. After reaching the citizens' pain threshold, people are going to start condemning armed actions and would like to put a quick end to war. The existence

of the civil control above military operations is always important and indispensable and this will be also one of the main attributes of the robotic warfare as well.

It is not so calming but true that the essence of a warfare is to convince the own population about the benefits and advantages of the planned armed actions and to break the opponent military forces and their society with psychological pressure. The outcome of a war depends on the casualties (death toll) that people still can tolerate. Military goals might be reached relatively fast but political win can be gained only long-term. The human factor is the most important part of the war since people decide, fight, support, assist and fall in a battle. Without real soldiers, wars would turn to a technology race that is not the historical essence of the armed conflicts. Since leading human factor is crucial, a complete robotic war is not real for now.

One of the most advanced representatives of a modern warfare is the swarm of drones that is more than a method. Swarm drones are reshaping the future of military operations, offering faster resupply, greater situational awareness and reduced risk for troops on the ground. The effectiveness of a swarm drone system comes from a combination of advanced software, intelligent networking and resilient hardware. Several core technologies work together to allow a swarm to operate as a coordinated, adaptive unit. AI-driven mission planning enables swarms to make collective decisions, allocate tasks and reorganise themselves mid-mission without human intervention. Real-time communication networks keep every drone aware of the swarm's position, health and objectives, ensuring seamless coordination during complex operations. If one drone drops out, data automatically reroutes through others.[37] Swarm drones are unquestionably able to increase the resilience of own troops but they can cause disproportional damages for the enemy that raises ethical questions as well.

I can state that there is a high need for new rules in the international law of warfare. The United Nations Organisation should be reformed in line with the new world order to be more effective than it is now. Now international law is relatively weak and many states violate its rules every day. Robotic warfare and its supposed less harsh impact on the civil society might be only a hypothetic shelter for global powers but this is only an illusion. Similar to conventional one's modern warfare also poses huge security challenges and risks for innocent civilians who are also exposed to violence (as during traditional operations) despite using precision weapons in robotic warfare.

References

1. ALWAYSAHEAD – OERLIKON AHEAD AIR BURST AMMUNITION; https://www.rheinmetall.com/Rheinmetall%20Group/brochure-download/

[37] Swarm Drones: Applications, Benefits, and Real-World Use Cases; https://bonvaero.com/swarm-drones-applications/ Downloaded: 7. April 2026

Weapon-Ammmunition/B038e0424-Oerlikon-Ahead-Air-Burst-ammunition.pdf Downloaded: 19. April 2026
2. Army Inks $1.2 Billion Deal to Equip Strykers with Short-Range Air Defense Weapons; October 02, 2020; https://www.military.com/daily-news/2020/10/02/army-inks-12-billion-deal-equip-strykers-short-range-air-defense-weapons.html Downloaded: 19. April 2026
3. Artificial Intelligence (AI) in Defence; https://defence-industry-space.ec.europa.eu/system/files/2025-12/Factsheet%20AI%20in%20Defence.pdf Downloaded: 19. April 2026
4. Asymmetrical warfare; https://www.britannica.com/topic/guerrilla-warfare/Origins-of-modern-guerrilla-warfare Downloaded: 4. April 2026
5. Autonomous Weapons; Slaughterbots are here. The era in which algorithms decide who lives and who dies is upon us. We must act now to prohibit and regulate these weapons. https://autonomousweapons.org/ Downloaded: 3. April 2026
6. Clausewitz: War as Politics by other Means; https://oll.libertyfund.org/pages/clausewitz-war-as-politics-by-other-means Downloaded: 19. April 2026
7. Cole Stryker, Eda Kavlakoglu: What is AI? https://www.ibm.com/think/topics/artificial-intelligence Downloaded: 10. April 2026
8. Defence: sustainability as a competitive advantage; 11 October 2024; https://www.gov.uk/government/publications/defence-sustainability-as-a-competitive-advantage/defence-sustainability-as-a-competitive-advantage Downloaded: 19. April 2026
9. Ensuring a national policy framework for artificial intelligence; Executive Orders; December 11, 2025; https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/ Downloaded: 10. April 2026
10. Francesco Tucci: Implications of the Industry 4.0 Concept On The Defence Sector; Military Technology Vol. XLVIII 1/2024; ISSN 0722-3226 p 37–39
11. George and Meredith Friedman: Future of War – Power, technology and American world dominance in the twenty-first century; St. Martin's Griffin, New York, 1996; ISBN 0-312-18100-0; Part 1: Weapons and Strategy (Introduction: The Culture of War and 1 David's Sling: On the Rise and Fall of Weapons; p 15–38
12. Heavenly forces for Italy; https://spartanat.com/en/heavenly-forces-for-italy Downloaded: 18. April 2026
13. How to Respond to Anti-Access/Area Denial (A2/AD)? Towards a NATO Counter-A2/AD Strategy; https://www.ndc.nato.int/fr/new-research-division-publication-how-to-respond-to-anti-access-area-denial-a2-ad-towards-a-nato-counter-a2-ad-strategy/ Downloaded: 7. April 2026
14. Ivan Zaccagnini: Emerging Technologies and the Enduring Elements of Warfare; STRATEGIC TRENDS 2026 – Key Developments in Global Affairs;

Center for Security Studies; https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/ST2026-C3-IZ.pdf Downloaded: 19. April 2026
15. Jatin Chawla: Cloud Computing in the Military; https://www.thegeostrata.com/post/cloud-computing-in-military Downloaded: 7. April 2026
16. Jennifer H. Swan: Air Force aims to gauge industry interest in making atomic clock to guide drone swarms; September 8, 2025; https://www.stripes.com/branches/air_force/2025-09-08/air-force-exploring-drone-swarm-capabilities-19018645.html Downloaded: 18. April 2026
17. Killer Robots (Human Watch Rights); https://www.hrw.org/topic/arms/killer-robots Downloaded: 3. April 2026
18. Marco Giulio Barone: The Continuing Evolutions of UGVs – Interview with Milrem Robotics; Military Technology Vol. XLVI Issue 3 2022, ISSN 0722-3226; p 76–77
19. Mia Fried: Economics of Warfare; https://sites.lsa.umich.edu/mje/2025/05/22/economics-of-warfare/ Downloaded: 19. April 2026
20. Mike Ball: Explosive Ordnance Disposal UGVs Delivered to UK MOD; 06 Jul 2021; https://www.unmannedsystemstechnology.com/2021/07/explosive-ordnance-disposal-ugvs-delivered-to-uk-mod/ Downloaded: 18. April 2026
21. Networked air defence – Oerlikon Skynex air defence system; https://www.rheinmetall.com/en/products/air-defence-systems/networked-air-defence-skynex Downloaded: 19. April 2026
22. PESTEL Analysis: What It Is and How to Use It for Strategic Planning; https://www.spiderstrategies.com/blog/pestel-analysis/ Downloaded: 7. April 2026
23. Prof. Tamar Hermann, Dr. Lior Yohanani, Yaron Kaplan: Most Jewish Israelis Think PM Netanyahu's Motivation in the War is Security Related; Most Arabs Think It's Personal; 30 March 2026; https://en.idi.org.il/articles/63856 Downloaded: 19. April 2026
24. Samuel Cranny-Evans: The Role of AI in Warfare; Military Technology Vol. XLVI Issue 1 2022, ISSN 0722-3226; p 56–57
25. Satellite Technology; https://starlink.com/technology Downloaded: 10. April 2026
26. Shane Schmid: What are programmable munitions and what advantages do they give to the military? https://www.slashgear.com/1925422/programmable-munitions-explained-how-benefit-military-advantages/ Downloaded: 7. April 2026
27. Stephen W Miller: Countering Tactical UAS and Loitering Munitions; Military Technology Vol. XLVI 3/2022; ISSN 0722-3226 p 26–31
28. Swarm Drones: Applications, Benefits, and Real-World Use Cases; https://bonvaero.com/swarm-drones-applications/ Downloaded: 7. April 2026
29. Swarm Intelligence – In subject area: Engineering; https://www.sciencedirect.com/topics/engineering/swarm-intelligence Downloaded: 7. April 2026

30. Swarming in Defense: How Autonomous Systems Transform Modern Operations; https://orbotix.tech/swarming-in-defense/ Downloaded: 19. April 2026
31. The Comprehensive Guide to Counter-UAS; https://www.dedrone.com/white-papers/counter-uas Downloaded: 9. April 2026
32. Thomas Anglero: The Future of Warfare: How AI and Robotics Are Redefining Global Security; March 19, 2025; https://www.anglewro.com/2025/03/19/future-of-warfare-how-ai-and-robotics/ Downloaded: 18. April 2026
33. Types of Military Robots: An In-Depth Analysis of Modern Robotic Warfare; https://www.kingsresearch.com/blog/are-military-robots-redefining-laws-of-war Downloaded: 31. March 2026
34. What is Anti-Access Area Denial Strategy; https://defensetalks.com/what-is-anti-access-area-denial-strategy/ Downloaded: 7. April 2026
35. What Is Cognitive Dissonance Theory? https://www.simplypsychology.org/cognitive-dissonance.html Downloaded: 19. April 2026
36. What is PESTEL Analysis? https://www.lumovest.com/library/management-strategy/pestel-analysis/ Downloaded: 18. April 2026
37. Zamzam Channa: Lethal Autonomous Weapon Systems: A Gamechanger Demanding Regulation; March 26, 2024; https://www.geopoliticalmonitor.com/lethal-autonomous-weapon-systems-a-gamechanger-demanding-regulation/ Downloaded: 18. April 2026

Éva Ladányi[1]

Exospheric Paradigm Shift: Integrating Orbital AI Networks, Quantum Security, and Modular Industrial Bases

Abstract:

The year 2026 represents a critical inflexion point in exospheric technological evolution. The convergence of interplanetary infrastructure, orbital artificial intelligence, and quantum security is currently forging a new systemic paradigm. This article examines recent advancements in Martian paleohydrological detection - specifically the deep-layer structures identified by the Perseverance rover's RIMFAX radar (Hamran et al., 2022) - alongside the strategic deployment of infrastructure on the lunar Farside (Burns et al., 2021). The latter remains a destination of paramount importance for deep-space observation due to its unique radio-quiet environment (National Geographic, 2026). This strategic significance is further underscored by the 2026 Artemis II mission, during which four astronauts performed the first human lunar flyby of the 21st century, providing critical direct observations of the Farside environment[2].

Orbital Digital Architecture and Quantum Security

Central to this transition is the emergence of an "orbital digital architecture." This framework integrates localised AI data processing – facilitated by the NVIDIA-based StarCloud constellation, with the long-range, unbreakable key distribution of quantum cryptographic systems (Yin et al., 2017; ESA, 2024). Leveraging the legacies of Micius, Jinan-1, and Eagle-1, this technological convergence establishes the foundational "Deep Space Internet", poised to serve as the future backbone of interplanetary communication and command (Wood et al., 2022; HVG, 2026).

Logistical Transformation and Industrial Autonomy

The study further evaluates the role of vertically integrated industrial complexes, most notably the TeraFab, in reshaping planetary logistics (iPon, 2026). AI-driven

[1] The author is an Honorary Assistant Professor at the Medical School of the University of Pécs (PTE ÁOK) and serves as the Co-Chair of the Space Working Group at HM EI Ltd., a strategic entity of the Hungarian Ministry of Defense. Holding advanced degrees in Theology, Canon Law, and Nuclear Energy Law, she is a recognized expert in state building and the hawala banking system, with extensive publications in these fields. Her interdisciplinary research focuses on the intersections of religious, legal, and security paradigms, and the strategic and public health impacts of irregular conflicts. Her work integrates agricultural sciences and complex biological systems.

[2] This crewed flight paved the way for the upcoming Artemis III landing mission, which will also carry the LEAF experiment.

manufacturing chains - ranging from semiconductor fabrication to the production of Starship fleet components - propose a new model of stability for global supply systems. Furthermore, the strategic implementation of battlefield additive manufacturing (3D-printed UAVs) illustrates a shift toward decentralised, on-site production, radically mitigating logistical vulnerabilities (DoD, 2025; Portfolio, 2026).

Sustainability and Regenerative Systems

Finally, we address the role of regenerative astrobiological systems, such as the LEAF experiment slated for Artemis III. These systems provide the biological prerequisites for the long-term sustainability of lunar and Martian outposts (NASA, 2024; Paul et al., 2022). Collectively, the 2026 technological landscape forms a unified ecosystem where geological exploration, quantum-based data integrity, and autonomous industrial capacity coalesce to define the conditions for a multi-planetary civilisation.

Keywords: Martian Exploration (RIMFAX), Artemis III, Artemis II, Lunar Infrastructure (Farside), Quantum Key Distribution (QKD), StarCloud, Orbital Edge AI, TeraFab Ecosystem, Additive Manufacturing, Regenerative Astrobiology.

Introduction: The Era of Interplanetary Infrastructure Development

The year 2026 represents a milestone in the history of astronautics: the era of prestigedriven technological demonstrations has come to an end, giving way to a period of systemlevel infrastructure development spanning multiple celestial bodies. Outer space is no longer an isolated domain of scientific exploration, but an extended, integrated operational environment for terrestrial industry, digital architecture, and biological survival strategies. Consequently, the central question of research has shifted from the mere capability of reaching the exosphere to the methodologies required for establishing sustainable, autonomous, and secure civilizational bases.

Beneath the Martian surface, the Perseverance rover's RIMFAX radar has revealed deeplayer fluvial structures that point to the planet's persistent hydrological cycles and former habitability (Hamran et al., 2022; Farley et al., 2020). In parallel, a new and critically important information infrastructure is emerging both in Earth orbit and on the lunar Farside. The vertical integration of artificial intelligence into satellite systems - exemplified by the StarCloud constellation's onboard AI algorithms - enables realtime orbital data processing, drastically reducing communication latency and bandwidth requirements.

At the same time, communication protocols grounded in the laws of quantum physics, such as Jinan1 built upon the Micius legacy and the European Eagle1 mission, are establishing the foundations of unbreakable data transmission. The systemlevel deployment of quantum key distribution (QKD) is not merely a technological innovation but the fundamental basis of future interplanetary data security.

The terrestrial industrial background is undergoing a similarly radical transformation. The TeraFab complex - which integrates processes ranging from semiconductor fabrication to the production of Starship fleet components into a single AIdriven vertical chain - introduces a new logistical model. This model no longer prioritises centralised mass production, but instead focuses on the rapid, scalable, and autonomous manufacturing of critical hardware elements required for maintaining planetary infrastructure.

This study aims to uncover the organic interconnections between Mars's geological past, the Moon's infrastructural future, and Earth's technological dominance. The technological landscape of 2026 indicates that humanity has entered the era of interplanetary infrastructure development, in which scientific discovery, digital sovereignty, and industrial autonomy converge into a single, coherent ecosystem.

Paleohydrological Reconstruction: Detecting Subsurface Fluvial Systems on Mars

The year 2026 has brought a decisive advancement in uncovering the early hydrological history of Mars. The latest data not only confirms the former presence of liquid water but also provides evidence for its longlasting, stable, and geologically active role. This insight fundamentally reshapes the scientific narrative surrounding the planet's past habitability.

The Perseverance Rover and the RIMFAX Technology: Revealing DeepLayer Fluvial Networks

The Radar Imager for Mars' Subsurface Experiment (RIMFAX), operating aboard the Perseverance rover, has enabled highresolution, noninvasive subsurface radar investigations of the multibillionyearold strata beneath the Jezero Crater. The instrument penetrated rock layers as old as 4.2 billion years, identifying an extensive, nowburied fluvial network (National Geographic, 2026; Stack et al., 2023) as well as a complex deltaic structure.

Based on the radar profiles, the early Martian surface was shaped not merely by episodic water flows but by longlasting river systems. The geometry and stratification of the detected sedimentary structures exhibit strong analogies to stable river valleys known from Earth.

Astrobiological Relevance: Persistent Water and the Possibility of Life (Paul et al., 2022)

One of the most significant implications of the RIMFAX data is that early Martian hydrological cycles were not limited to short, catastrophic flooding events. The presence of persistent water flows:

– increases the likelihood of prebiotic chemical processes,
– provides a longer temporal window for the emergence of microbial life,
– and creates a stable environment conducive to the hypothetical onset of biological evolution.

This realisation gives new momentum to astrobiological research, particularly the Jezero Crater samplereturn program (Mars Sample Return), expected in the early 2030s.

Infrastructure and Radiation Protection: Natural Shielding for Future Martian Bases

The significance of subsurface fluvial structures extends beyond reconstructing the planet's past. Buried channels and the thick overlying regolith layers provide natural passive radiation shielding against highenergy cosmic rays. This is especially important for future human expeditions, as:

– surface radiation levels on Mars exceed those on Earth by several multiples,
– subsurface cavities and paleochannels offer ideal locations for longterm habitat modules (NASA, 2023),
– and they support insitu resource utilisation (ISRU) operations, such as waterice extraction or the production of local construction materials.

Thus, paleohydrological reconstruction is not merely a scientific endeavour but also a strategic foundation for planning future Martian colonisation.

Strategic Reorientation: The Scientific and Geopolitical Elevation of the Lunar Farside

Image 1: The far side of the Moon (Farside) as seen by the Orion spacecraft's camera during the Artemis II mission (2026). Due to the region's radio-quiet environment, it is of particular importance for deep-space cosmological observations and quantum communication infrastructure. Source: Getty

By 2026, a clear strategic shift has emerged in the history of lunar exploration: the earlier phase of technology demonstrations focused primarily on the near side has been replaced by targeted, infrastructuredriven development of the lunar Farside. The Farside's unique geophysical characteristics-most notably the absence of a direct lineofsight to Earth-provide natural shielding that creates a radioquiet environment unparalleled in the Solar System (Burns et al., 2021). This region has become not only a scientific focal point but also one of the most important locations for deepspace observations, quantum communication, and geopolitical positioning.

Protecting the RadioQuiet Environment: A New Gateway to DeepSpace Cosmology

The Moon's mass effectively blocks Earth-originating anthropogenic radio-frequency interference (RFI), making the Farside the only natural laboratory where ultra-low-frequency (ULF) bands, particularly those below 30 MHz, can be observed without disturbance. These frequencies are inaccessible from Earth due to the filtering effect of the ionosphere.

Interferometric networks deployed on the Farside aim to:

- detect hydrogenline emissions from the universe's "Dark Ages",
- map early cosmic structure formation,
- and refine cosmological models.

Protecting the radioquiet zone is therefore not only a scientific priority but also a strategic interest involving the Artemis program, China's Chang'e missions, and multiple international consortia.

Quantitative Geological Investigations in the South Pole-Aitken Basin (Wu et al., 2024): Insights into the Moon's Interior

The Moon's South Pole-Aitken (SPA) Basin is one of the largest and oldest impact structures in the Solar System. International missions in 2026 - including Chang'e7, Chang'e8, and preparatory Artemis programs - are conducting in situ spectroscopic and geophysical measurements that:

- provide direct information on the composition of lunar mantle material,
- support the reconstruction of the Moon's early differentiation processes,
- and offer new data for understanding the impact history of the inner Solar System.

Due to its unique topography and geological heterogeneity, the SPA Basin is one of the most important scientific targets on the Farside and a potential site for future lunar bases.

RelayBased Communication Architecture: The Backbone of Farside Operations (NASA, 2023)

One of the greatest challenges of the Farside is the lack of direct communication with Earth. To address this, by 2026, a relay constellation has been established around the Earth-Moon L2 Lagrange point, beginning with Queqiao2 and followed by nextgeneration relay satellites.

These systems:

- ensure continuous data connectivity between Farside surface assets and Earth,
- form a multinode, protocolagnostic communication network,
- and provide the foundation for future autonomous surface operations (robotics, ISRU, navigation).

The relay architecture is not merely a technical necessity but a key element of strategic control over the lunar Farside.

Digital Sovereignty and Security Architecture: Integrating SpaceBased Data Centres and Quantum Communication

The longterm sustainability of lunar and deepspace bases requires an information infrastructure capable of providing high computational capacity, lowlatency decisionmaking, and unbreakable data security. In the technological landscape of 2026, these requirements rest on two mutually reinforcing pillars: orbital edge computing and quantumbased key distribution (Quantum Key Distribution, QKD). The integration of these technologies forms the foundation of the future interplanetary communication and control system.

StarCloud and the Transformation of Orbital Data Processing (HVG, 2026; Moreira-Shneider-Hein, 2023)

The StarCloud constellation-a network of satellites equipped with NVIDIAbased highperformance GPUs-fundamentally reshapes the paradigm of satellite data management. In earlier models, satellites functioned primarily as datacollection units, transmitting raw data to Earth for processing. In contrast, StarCloud:

- executes artificial intelligence algorithms onboard,
- performs realtime segmentation, classification, and anomaly detection,
- reduces required bandwidth by as much as 80-90%,
- and minimizes decisionmaking latency.

This capability is particularly critical for autonomous robotic operations on the lunar Farside, where communication latency and bandwidth are inherently limited. StarCloud thus functions not merely as a dataprocessing system but as the backbone of future orbital AI infrastructure.

Quantum Cryptographic Networks and the Protection of Data Integrity (Yin et al., 2017; Chen et al., 2021; ESA, 2024)

The global escalation of cybersecurity threats has made it necessary to adopt communication protocols grounded in the laws of physics and theoretically unbreakable (ESA, 2024). Quantum key distribution (QKD) systems - building on the pioneering achievements of Micius (2016) - reached the stage of systemlevel implementation by 2026.

The most significant developments include:

- **Jinan1 (China):** a longdistance, satellitebased QKD demonstration integrated into the Chinese quantum backbone network.
- **Eagle1 (Europe):** launched in 2026 as part of the EuroQCI program, initiating the construction of a panEuropean quantum communication infrastructure.
- **BRICS Quantum Network:** a multinational initiative emphasising the geopolitical significance of quantum communication.

The essence of QKD lies in the fact that any external disturbance of the quantum state of entangled photons is immediately detectable, making eavesdropping physically impossible without leaving a trace. This property establishes quantum communication as the cornerstone of future interplanetary data security.

Global Network Convergence and Strategic Stability

By 2026, quantum communication has moved beyond national frameworks and is trending toward the formation of a hybrid orbitalterrestrial infrastructure. Its main components include:

- satellite relays for longdistance data transmission,
- suborbital and orbital quantum nodes to guarantee security,
- terrestrial quantum backbone networks (EuroQCI, the Chinese quantum network),
- interoperable protocols enabling the unification of interplanetary data traffic.

This convergence is not merely a technological development but also a factor of strategic stability. Future interplanetary governmental, commercial, and scientific data flows will rely on systems that are:

- autonomous,
- physically protected,
- and decentralised.

Digital sovereignty thus acquires not only a terrestrial but also an exospheric dimension.

Industrial Transformation and Logistical Autonomy: The TeraFab Ecosystem and Portable Additive Manufacturing Technologies

By 2026, deepspace expansion and modern battlefield requirements have exerted such intense technological and logistical pressure on global industry that a radical shift in manufacturing paradigms has become necessary. The emphasis has moved away from centralised mass production toward vertically integrated, highcapacity industrial complexes (iPon, 2026; HVG, 2026) and decentralised, onsite additive manufacturing solutions (Portfolio, 2026). This dual model simultaneously serves the rapidly evolving needs of interplanetary infrastructure development and modern warfare.

The TeraFab Project and Vertical Integration: A New Generation of Industrial Ecosystems

The 20billiondollar TeraFab investment, developed under the direction of Elon Musk, has created a multifunctional industrial ecosystem capable of serving the synergistic needs of Tesla, SpaceX, and xAI. The significance of TeraFab lies in its ability to integrate:

- semiconductor manufacturing,
- batterycell production,
- structural component casting,
- and vehicle and aerospace assembly lines

into a single, AIdriven vertical chain.

This model not only increases costefficiency but also:

- minimises supplychain vulnerability,
- accelerates the production of critical hardware elements,
- and enables the serial manufacturing of components required for interplanetary missions (e.g., Starship fleet elements, Martian ISRU modules, lunar robotic units).

TeraFab is thus the first industrial complex of the 21st century explicitly optimised for the demands of planetary logistics.

Battlefield Additive Manufacturing: The Realisation of "JustinTime"-Tactical-Autonomy

In 2026, the United States Department of Defence and its allied partners introduced a form of "Just-in-Time" tactical logistics based on high-precision 3D-printing units deployed at the front line or at remote expeditionary bases. These mobile manufacturing platforms enable:

– The on-site production of unmanned aerial vehicles (UAVs);
– Rapid adaptation of drones to current threat levels;
– Immediate replacement of damaged or obsolete components;
– A drastic reduction in the risks associated with logistical supply routes.

Decentralised additive manufacturing has thus become one of the most important innovations in modern warfare, prioritising tactical autonomy and rapid responsiveness.

Global Security Policy Dimensions: The Dual Nature of Technological Dominance (HVG, 2026)

The geopolitical events of 2026 - including Iran's demonstration of next-generation ballistic delivery systems and the deployment of U.S. and allied satellite-based radar systems in response - highlight the dual nature of technological dominance:
– In terrestrial conflicts, rapid manufacturing capacity and on-site adaptation provide decisive advantages;
– In exospheric resource competition, vertically integrated industrial bases constitute the strategic hinterland.

TeraFab-type complexes and mobile additive manufacturing units together form the technological - infrastructural foundation that will shape the balance of power in the mid-21st century - whether in terms of Earth's geopolitical stability or the exploitation of lunar and Martian resources.

Astrobiological Validation and Bioregenerative Life Support Systems

One of the most critical prerequisites for sustained lunar presence and future Martian expeditions is the drastic reduction of dependence on Earth's biosphere. In this respect, the year 2026 marks a turning point: research has shifted from theoretical modelling and laboratory experiments toward biological validation conducted in real extraterrestrial environments. The focus is on the edaphic, radiation-biological, and ecological factors that determine whether plant and microbial life can adapt to the extreme conditions of the Moon and Mars.

The LEAF Project and the Foundations of Lunar Agriculture (NASA, 2024)

The LEAF (Lunar Effects on Agricultural Flora) experiment, coordinated by NASA, is one of the key scientific modules of the Artemis III mission. LEAF is the first controlled biological experiment that directly examines the dynamics of plant photosynthesis and transpiration on the lunar surface, analyses the long-term

effects of lunar gravity (0.16 g), and maps plant stress responses to the complex spectrum of cosmic radiation.

The aim of the experiment is not only to determine whether plants can survive in the lunar environment but also to identify the physiological adaptation mechanisms that enable stable biomass production. The results of LEAF will be fundamental for designing future lunar greenhouses, bioregenerative modules, and ISRU-based agricultural systems.

Genetic Adaptation and Selection: The Plant Genome's Response to the Exospheric Environment

The selection of experimental organisms, including *Arabidopsis thaliana* and *Wolffia* (duckweed), is a deliberate strategic choice (Paul et al., 2022). These species have short life cycles, possess fully characterised genomes, and are ideally suited for tracking epigenetic changes.

The goal of the research is to identify and cultivate plant varieties that can produce stable biomass even on regolith-based substrates, tolerate high radiation exposure, and provide sustainable oxygen and food sources for long-term bases. The study of genetic adaptation is therefore not merely an agronomic question but a foundational element of biological survival strategies on the path toward a multi-planetary civilisation.

Closed-Loop Ecological Systems (ECLSS): Foundations of Regenerative Life Support (Wheeler, 2017)

The role of plant cultivation extends far beyond food production. The life-support systems of future lunar and Martian bases increasingly rely on closed-loop ecological systems (ECLSS), in which plants stabilise the carbon-dioxide-oxygen cycle, contribute to water recovery, and reduce the load on mechanical-chemical filtration systems.

Integrating biological components increases system redundancy, reduces the need for external resupply, and improves long-term survival prospects. Thus, the experiments conducted in 2026 examine not only plant behaviour in extreme environments but also the symbiosis between biological and technological systems-an essential requirement for the operation of future interplanetary bases.

Synthesis and Outlook: The Convergence of Technological Singularity and Interplanetary Infrastructure

An analysis of the events and technological developments of 2026 makes it clear that humanity has moved beyond the isolated, experimental era of space exploration. Martian paleohydrological research, infrastructure development on the lunar Farside, and

advances in quantum-information security architectures have coalesced into a unified, integrated technological ecosystem. This ecosystem is no longer merely a domain of scientific discovery but the foundational structure of an interplanetary civilisation.

New Dimensions of Information Sovereignty: The Emergence of the Deep Space Internet (HVG, 2026; ESA, 2024)

The integration of NVIDIA-based orbital computing capacity (StarCloud) with quantum key distribution (QKD) represents not just a technological advancement but a breakthrough of civilizational significance. The synergy between these systems establishes the foundations of the Deep Space Internet - a communication protocol architecture in which:

- Data processing occurs locally on orbital AI systems;
- Encryption is grounded in the laws of physics;
- Communication channels are interference-free;
- The network is decentralised, redundant, and self-healing.

The lunar Farside, with its radio-quiet environment and relay constellations, becomes the primary node of this network. The civilisation or alliance that controls this node gains a strategic advantage in interplanetary governance, commerce, and scientific data exchange.

Industrial and Logistical Paradigm Shift: The Era of Decentralised Manufacturing (iPon, 2026; Portfolio, 2026)

The proliferation of the TeraFab model and frontline additive manufacturing technologies radically rewrites the theory of global and exospheric supply chains. Centralised mass production is being replaced by "Just-in-Time" on-site resource allocation, which manifests as regolith-based construction on the Moon, deployment of ISRU modules on Mars, and tactical autonomy on Earth.

This flexibility is not merely an economic advantage but one of the cornerstones of 21st-century geopolitical and astropolitical stability. The maintenance of interplanetary infrastructure is possible only with systems that adapt rapidly, can be manufactured locally, and require minimal external resupply. TeraFab and mobile additive manufacturing units together form the technological hinterland that will shape the balance of power in the coming decades.

Biological and Technological Symbiosis: A New Generation of Life-Support Systems (NASA, 2024; Paul et al., 2022)

Astrobiological validation processes, such as the LEAF project, highlight that technological expansion is unsustainable without the adaptive extension of the biosphere.

Through AI-driven closed-loop ecological systems (ECLSS) and targeted genetic selection, humanity becomes capable of the in-situ utilisation of local resources (regolith, water ice, minerals), stable production of plant biomass, and the maintenance of long-term oxygen and water cycles.

This biological-technological symbiosis constitutes the biological prerequisite for becoming a multi-planetary civilisation. Future bases will not merely be technological installations but living, self-sustaining ecosystems capable of adapting to environmental change.

Summary

The technological and scientific developments of 2026 make it clear that humanity has entered the era of interplanetary infrastructure construction. The research and industrial domains presented in this study-Martian paleohydrological reconstruction, the strategic elevation of the lunar Farside, the integration of orbital artificial intelligence and quantum communication, and the emergence of vertically organised industrial and biological systems-coalesce into a coherent, mutually reinforcing technological ecosystem.

The discovery of deep-layer fluvial networks on Mars offers new insight into the planet's habitability potential, while the lunar Farside is becoming the primary hub for deep-space observations and interplanetary communication. In parallel, the TeraFab model and decentralised additive manufacturing technologies are radically transforming global and exospheric supply chains. Locally producible infrastructure constitutes one of the key elements of 21st-century geopolitical and astropolitical stability. Finally, the integration of biological systems through the LEAF project and ECLSS highlights that technological expansion can only be sustainable through the adaptive extension of the biosphere, turning future bases into living, self-sustaining ecosystems.

References

Mars Research and Palaeohydrology

1. Farley, K. A., et al. (2020). Mars 2020 Mission Overview. *Space Science Reviews,* 216(8).
2. Hamran, S. E., et al. (2022). RIMFAX: A Ground-Penetrating Radar for the Perseverance Rover. *Journal of Geophysical Research: Planets*, 127(3).
3. Stack, K. M., et al. (2023). Sedimentology and stratigraphy of the lower delta sequence, Jezero crater, Mars. *Science Advances*, 9(14).
4. National Geographic. (March 2026). *Betemetett folyórendszert találtak a Marson*. National Geographic Online.

Lunar Research, Farside, and Radio-Quiet Zones
1. Burns, J. O., et al. (2021). Transformative science from the lunar Farside: observations of the dark ages and exoplanetary systems at low radio frequencies. *Philosophical Transactions of the Royal Society A,* 379(2188). https://doi.org/10.1098/rsta.2019.0564
2. Wu, W. R., et al. (2024). Lunar Farside samples returned by Chang'E-6 mission: significance for understanding the South Pole-Aitken Basin stratigraphic history. *Planetary and Space Science,* 230.
3. NASA. (2023). *Artemis Program: Science Definition Report*. NASA Technical Reports Server.

Quantum Communication and QKD
1. Yin, J., et al. (2017). Satellite-Based Entanglement Distribution Over 1200 km. *Science,* 356(6343), 1140–1144.
2. Chen, Y. A., et al. (2021). An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature,* 589, 214–219.
3. European Space Agency. (2024). *Eagle-1 Quantum Key Distribution Mission Overview*. ESA Publications.

Orbital AI and StarCloud
1. Moreira, C. M., Shneider, C., & Hein, A. M. (2023). Edge computing in space: Design of an FPGA architecture for thermal anomaly detection based on a machine learning approach. *Acta Astronautica,* 204, 567–580.
2. HVG. (March 17, 2026). *StarCloud: NVIDIA-processzoros műholdas adatközpont mesterséges intelligenciával*. HVG Technika.
3. Prohardver. (2026). *A világűrbe repíti az AI-t az NVIDIA és a Starcloud*. https://prohardver.hu/hir/nvidia_x_starcloud_ai_adatkozpont_vilagur.html

Industrial Integration, TeraFab, and Additive Manufacturing
1. Gibson, I., et al. (2021). *Additive Manufacturing Technologies*. Springer Nature.
2. iPon. (March 2026). *Elon Musk elindítja a 20 milliárd dolláros TeraFab projektet*. iPon Tech News.
3. Portfolio. (March 25, 2026). *Váratlan húzás az Egyesült Államoktól: a frontvonalon is kinyomtatható az új drón*. Portfolio Globál.
4. HVG. (March 23, 2026). *Elon Musk TeraFab: saját chipgyártás és SpaceX-Tesla-xAI integráció*. HVG Gazdaság.

Astrobiology, LEAF, and ECLSS
1. Wheeler, R. M. (2017). Agriculture for Space: People and Places Paving the Way. *Open Agriculture,* 2, 14–32.

2. Paul, A. L., et al. (2022). Plants grown in Apollo lunar regolith present stress-associated transcriptomes that inform prospects for lunar exploration. *Communications Biology*.
3. De Micco, V., et al. (2023). Perspectives for plant biology in space and analogue environments. *npj Microgravity,* 9, Article 67.
4. NASA. (2024). *LEAF Experiment Overview for Artemis III*. NASA Science Mission Directorate.

Eszter Réka Gyaraki Dr.[1]:

Why are people susceptible to Manipulation in Cyberspace? Social Engineering as an Attack Vector

Abstract:

So-called identity theft can be considered one of the most significant precursors to online fraud. These phenomena effectively provide a kind of "cloak of invisibility" for perpetrators-including criminals and even terrorists-as they allow them to remain hidden from authorities by using someone else's identity. At the same time, identity theft poses a serious risk not only on an individual level but also threatens both public safety and national security on a broader scale.

For law enforcement, identity theft is by no means a new crime. For decades, they have encountered cases where perpetrators produce or use forged identification documents. These cases can be extremely diverse: ranging from simple document forgers to so-called identity thieves, all the way to individuals who, for various reasons-such as seeking asylum-are forced to assume a different identity.

Keywords: social engineering, fraud, cybercrime, identity-fraud

Introduction

In contemporary society, it is virtually inconceivable to conduct everyday activities without the Internet, as it offers the fastest, simplest, and most convenient means of handling affairs at any time and from any location. Public institutions increasingly rely on digital platforms to communicate with citizens, thereby reducing face-to-face interactions and unnecessary waiting times.

Parallel to the advancement of digital technologies, cybercrime has also become increasingly sophisticated because a new, non-physical domain has emerged. One of the most important factors behind the success of cybercrime, however, is not purely technical; rather, it is rooted in human manipulation. Social engineering refers to a set of manipulative techniques aimed at persuading victims to disclose sensitive information voluntarily or to perform harmful actions.

The effectiveness of such attacks is closely linked to the characteristics of human psychology, since decisions are often shaped not by rational analysis alone but by emotions, habits, and social norms. Cybercriminals systematically exploit these

[1] Dr. Réka Eszter Gyaraki PhD., police Major, Associate Professor, National University of Public Service, Faculty of Law Enforcement, Department of Cybercrime

mechanisms in the digital environment. The aim of this study is therefore to examine the psychological factors that make social engineering attacks effective and to identify possible methods of prevention.

The Arena of Fraud in the Age of the Fourth Industrial Revolution

With the rise of the Internet, cyberspace has become a new arena for fraudulent activity. This development is driven by the continuously growing number of users and by information systems designed to meet the demands of a rapidly changing world. Online marketplaces and advertising platforms are accessible at any time and from any location, including those integrated into social media, where users participate in geographically or socially defined buying and selling groups.

There is a significant difference between crimes committed in physical space and those committed in cyberspace. In physical environments such as shopping centres or entertainment venues, offenders and victims are more likely to encounter one another directly because these spaces attract large numbers of people. In such settings, surveillance systems and the possibility of personal identification increase the likelihood of detection. By contrast, in cyberspace offenders and victims rarely, if ever, meet in person; transactions and interactions take place through virtual marketplaces.

Whereas victim selection in physical space is often facilitated by visible carelessness, such as leaving valuables unattended or being distracted in a crowd, irresponsibility in virtual environments takes different forms. Even highly cautious individuals may become victims of cybercrime.

There are numerous reasons why offenders commit cyber-related crimes: the prospect of rapid financial gain; the low marginal cost of online activities due to global accessibility; the reduced effectiveness and higher expense of law-enforcement detection; slower and less frequent criminal procedures due to international legal complexity; difficulties in identifying offenders and their locations; the expansion of international trade and communication; and the latent nature of many cybercrimes, which may remain undetected for long periods.

Before the advent of email, fraudsters had to contact each potential victim individually by post, fax, telephone, or direct personal interaction. These methods were resource-intensive and made victim selection more difficult. The digital environment has significantly improved offenders' chances of reaching susceptible victims because they can conduct preliminary research through social media platforms, online groups, and dating websites before initiating contact.

Deception in the Information Technology Environment

Computer-related fraud and deception may generally be divided into two principal groups. First, there are financially motivated frauds in which direct pecuniary harm

is observable and the offender's primary motivation is monetary gain rather than information acquisition. Such cases include advance-fee scams, counterfeit product offers, and fraudulent prize notifications.

Second, there are personal-information-seeking frauds in which the unlawful conduct is directed primarily at obtaining personal data, although financial gain may also be a secondary objective. Examples include malware attacks, phishing emails, and fake websites. In such cases, the acquired data may be used to commit further offences.

A third category may also be distinguished, although it departs somewhat from classical fraud patterns. Here, offenders acquire and misuse personal information such as names or photographs for deceptive social interaction, identity misuse, or sexually exploitative purposes on social and dating platforms.

Illegal Financial Gain in Cyberspace

The widespread proliferation of fraud in cyberspace is closely linked to the popularity of e-commerce. Products advertised through online marketplaces, including those embedded in social media, are often offered at attractive prices and may involve goods that are highly desirable or difficult to obtain.

The seriousness of economic cybercrime is illustrated by data from the FBI's Internet Crime Complaint Center, which reported 301,580 complaints in 2017 with losses exceeding USD 1.4 billion[2]. The anonymity, speed, and transnational nature of cyberspace contribute significantly to the persistence and effectiveness of these offences.

Online Fraud, Social Engineering, and Human Manipulability in the Digital Environment

Online Fraud

With the expansion of the Internet, traditional marketplaces have increasingly been replaced by online commerce, which has not only reproduced conventional forms of fraud but has also introduced new opportunities derived from the cyber environment.

In online transactions, buyers rarely have the opportunity to inspect a product in person; at best, they may request photographs or additional information. As a result, transactions often depend on mutual trust, whether goods are exchanged for other goods or for money. This structural distance increases the risk of deception: the advertised item may not exist, may differ substantially from its description, or may never be delivered at all. At the same time, sellers are also exposed to risk, for

[2] IC3: Internet Crime Report 2018 (https://www.ic3.gov/AnnualReport/Reports/2018_ic3report.pdf)

instance when payment is made with stolen credit-card data. The broader growth of cyber-enabled fraud is closely associated with the rise of e-commerce and the increasing scale of Internet-facilitated crime (FBI IC3, 2018).

Victim behaviour also plays an important role in the success of online fraud. In many cases, the suspiciously low price of the advertised product should itself raise concerns, yet consumers may ignore such warning signs because of convenience, urgency, or the prospect of a bargain. Research in cognitive psychology suggests that under uncertainty, individuals often rely on mental shortcuts rather than detailed analytical assessment, which makes them more susceptible to manipulation in digital settings[3].

Foundations of Social Engineering

A proper understanding of social engineering requires close attention to the psychological mechanisms that shape human behaviour. The manipulative techniques used by cybercriminals are not random; rather, they are built on well-established and empirically documented patterns of influence and decision-making. Human judgment is frequently guided by heuristics, that is, mental shortcuts that enable rapid responses but do not always produce reliable conclusions.

One of the most influential scholars of persuasion, Robert Cialdini, identified key principles that significantly shape human behaviour, including authority, scarcity, reciprocity, and social proof[4]. These principles are adaptive in everyday life because they help people navigate complex social situations efficiently. In manipulative contexts, however, they become sources of vulnerability.

The principle of authority explains why individuals are more likely to comply with requests that appear to come from a bank, government agency, employer, or other legitimate institution. Scarcity increases the perceived value of limited-time opportunities, while social proof encourages individuals to follow what they believe others are doing. Social engineering attacks routinely weaponize these tendencies in order to prompt victims to disclose confidential information or perform harmful actions[5].

According to Kahneman's dual-process model, human cognition operates through two interacting systems: a fast, intuitive, automatic process and a slower, more analytical and reflective process[6]. Social engineering attacks are typically designed to trigger the fast system through urgency, fear, authority cues, or emotional stimulation, thereby bypassing more deliberate forms of reasoning.

[3] Daniel Kahneman: Thinking, fast and slow (New York, 2011)

[4] Cialdini, Robert B.: Influence, New and Expanded: The Essential Guide to the Psychology of Influence and Persuasion in Everyday Life, 2021 (2009)

[5] Kahneman

[6] Kahneman

Phishing

Phishing remains one of the most widespread and consequential manifestations of social engineering. It involves deceptive communication intended to induce individuals to reveal sensitive information, click on malicious links, or install harmful software. These attacks frequently impersonate trusted institutions such as banks, utility providers, telecommunications companies, or government bodies, and may be delivered via email, text message, telephone call, or fraudulent websites[7].

Contemporary phishing attacks are increasingly sophisticated. Earlier indicators of fraud, such as poor grammar or the mere absence of HTTPS, are no longer reliable warning signs. Highly targeted phishing, often referred to as spear phishing, is substantially more effective than generic mass phishing because it draws on personal information gathered from publicly available sources, especially social media[8].

Synthetic Identity Fraud

Synthetic identity fraud refers to the creation of fictitious identities by combining genuine personally identifiable information with fabricated data. These hybrid identities may be used to obtain financial products, open accounts, or conduct other fraudulent activities. The U.S. Federal Reserve has described synthetic identity fraud as a major and fast-growing threat within the payments ecosystem because such identities are difficult to detect and may cause substantial losses[9].

Work-at-Home Fraud

Work-at-home scams exploit economic vulnerability and the hope of rapid financial improvement by offering seemingly legitimate remote employment opportunities. Victims may be asked to provide personal data, recruit additional individuals, sell overpriced products, or pay registration fees or deposits, yet they receive nothing of value in return. Such schemes frequently remain latent because victims may be reluctant to report them, especially if they believe they have signed a valid agreement or have lost only a relatively small amount.

Romance Fraud

Romance scams rely on emotional manipulation. Offenders initiate contact through email or social media, often presenting themselves as socially respected professionals such as doctors, military personnel, or offshore workers. After building trust and emotional dependence, they begin requesting money for travel, medical treatment,

[7] ENISA Threat Landscape 2023

[8] Tom Jagatic, Nathaniel Johnson, Markus Jakobsson, and Filippo Menczer: Social Phising (Communications of the ACM, Volume 50, Issue 10, 2007) 94-100

[9] Board of Governors of the Federal Reserve System 2019 (forrás: https://www.federalreserve.gov/publications/2019-ar-overview.htm)

visas, or other fabricated needs. The FBI's reporting categories continue to show that confidence and romance fraud generate substantial losses and cause severe psychological harm in addition to direct financial damage[10].

CEO Fraud and the Legal Assessment of Deception

One of the most well-known institutional forms of social engineering is so-called CEO fraud, also widely discussed under the broader category of business email compromise. In such cases, the attacker impersonates a senior executive and instructs an employee to execute an urgent and confidential financial transfer. These attacks are especially effective because they combine authority, urgency, and secrecy, thereby suppressing verification behaviour[11].

The legal assessment of such cases is complex. On the one hand, the conduct reflects fraud because the offender intentionally deceives the victim for unlawful financial gain. On the other hand, questions of organisational responsibility may arise where the victim organisation lacks adequate internal controls, such as multi-level approval mechanisms for financial transactions.

The Psychological Operation of Social Engineering Techniques

The effectiveness of social engineering lies in the attacker's ability to activate several psychological mechanisms simultaneously. Phishing messages, for example, often combine appeals to authority, urgency, fear, and curiosity in a single communication. Such messages may warn that an account will be suspended, that a payment has failed, or that immediate confirmation is required to avoid serious consequences. These cues generate strong emotional responses and reduce the likelihood of reflective analysis[12].

Another common form of social engineering is pretexting, in which the attacker constructs a plausible scenario in order to obtain trust and cooperation. For instance, an offender may impersonate an IT specialist, bank employee, lawyer, or public official and use that role to request credentials, files, or access permissions. This method is particularly effective because it exploits social norms of helpfulness, cooperation, and compliance with authority[13].

[10] FBI IC3 Annual Report Released -Report Shows Cyber-Enabled Crimes and Costs Rose in 2018 (2019, forrás: https://www.fbi.gov/news/stories/ic3-releases-2018-internet-crime-report-042219)

[11] Verizon 2024 Data Breach Investigations Report

[12] Kahneman

[13] Christopher Hadnagy: Social Engineering: The Science of Human Hacking. 2nd Edition, Wiley. 2018

The digital environment has also introduced new forms of manipulation. Artificial intelligence can generate highly personalized messages, imitate tone and style, and adapt communication dynamically. Deepfake technologies further enable voice- and video-based impersonation, thereby increasing the persuasive force of authority and trust cues[14].

Legal Assessment and Regulatory Challenges

A defining feature of social engineering is that, unlike many classical cybercrimes, it does not primarily exploit technical vulnerabilities but rather human ones. This creates difficulties for legal classification because traditional categories such as unauthorized access or hacking do not always apply neatly when victims disclose information voluntarily, even though they do so under deception.

In European legal systems, including Hungarian criminal law, such conduct may therefore be prosecuted through a combination of offences, such as fraud, computer-related fraud, unlawful data acquisition, or misuse of personal data, depending on the specific facts of the case. At the EU level, Directive 2013/40/EU provides a harmonized framework concerning attacks against information systems, while the Budapest Convention remains the leading international treaty for cybercrime cooperation (European Parliament and Council, 2013; Council of Europe, 2001).

The General Data Protection Regulation (GDPR) is also highly relevant. Where a successful social engineering attack leads to unauthorized disclosure or exfiltration of personal data, the incident may qualify as a personal data breach, potentially resulting in significant regulatory consequences for the affected organisation (European Parliament and Council, 2016).

Cross-border enforcement remains one of the most difficult aspects of cybercrime regulation. Europol, particularly through the European Cybercrime Centre, plays an important role in coordinating information exchange and supporting joint investigations among Member States (Europol, n.d.).

Evidentiary Difficulties

A distinctive characteristic of social engineering is that the victim becomes an active participant in the attack, which complicates evidentiary assessment. Investigators must reconstruct the communication process, demonstrate deception, and prove the offender's intent. This is particularly difficult in cases involving anonymized or encrypted communication. Because phishing, smishing, and vishing increasingly rely on professional language and convincing visual design, distinguishing genuine from fraudulent communication may itself require expert analysis[15].

[14] ENISA 2023
[15] ENISA 2023

Modern Challenges in the Field of Social Engineering

Social engineering has become progressively more complex alongside the development of the information society. Whereas early attacks were based primarily on simple deception, contemporary attacks combine psychological manipulation with advanced technological tools. Their evolution can be divided into several stages linked closely to changes in the technological environment.

In the early stage, from the 1990s to the early 2000s, attacks were relatively simple and often consisted of generic mass messages containing obvious errors. In the next stage, the spread of social media and online data-sharing enabled attackers to gather detailed information about potential victims, which gave rise to spear phishing and other targeted attacks[16].

From the second half of the 2010s onward, social engineering entered a phase marked by automation and professionalization. Organised groups increasingly offered tools and infrastructure as services to other criminals, resulting in models such as phishing-as-a-service. Today, the newest stage of development is shaped by artificial intelligence, which enables real-time adaptation and high levels of personalization[17].

Artificial Intelligence and Automated Attacks

Artificial intelligence has fundamentally transformed the methods of social engineering. AI systems can process large volumes of data rapidly, allowing attackers to construct detailed profiles of victims that include not only demographic information but also behavioural patterns, communication style, and areas of interest. On this basis, attackers can generate highly credible messages that closely match the target's communicative environment.

Automation also allows attackers to reach large numbers of targets simultaneously with minimal resource expenditure. As a result, attacks become faster, more economically efficient, and more scalable, thereby contributing to the broader spread of cybercrime[18].

Deepfakes and Advanced Identity Manipulation

Deepfake technology has elevated social engineering attacks to a new level. Through machine learning, attackers can generate false audio and video materials that imitate the appearance and speech patterns of real persons with a high degree of realism. This is especially dangerous because individuals tend to place strong trust in visual and auditory signals. In corporate settings, attackers may imitate executives

[16] Jagatic et al., 2007
[17] ENISA, 2023; Verizon, 2024
[18] ENISA, 2023; Verizon, 2024

and issue instructions regarding financial transactions, thereby causing significant economic damage[19].

According to Csaba Krasznay, deepfake technology is particularly well-suited to causing social panic, especially in tense wartime or crisis situations. During the Russia-Ukraine war, for example, a doctored video appeared in March 2022 in which Ukrainian President Volodymyr Zelenskyy appeared to be announcing a ceasefire to Ukrainian troops. The rapid spread of such a manipulated recording on social media is capable of causing immediate panic and complete chaos among both the civilian population and the armed forces; therefore, strategic communication and a swift official rebuttal are essential to avoid negative consequences.

In my view, inciting social panic has become perhaps the most effective tool of today's hybrid warfare. The logic behind instilling panic is that it turns the population into a weapon.

In an artificially created crisis situation (be it a false alarm about a radiation threat or the collapse of the banking system), the irrational behavior of the deceived masses has an immediate physical impact. Road blockages caused by mass exodus, or a financial collapse triggered by a bank run, can in and of themselves be enough to paralyze a state's functioning. The attacker does not even need to strike the target physically; society collapses under its own weight.

Legal and Regulatory Challenges

The pace of technological development poses a serious challenge for legislators. Existing legal frameworks frequently struggle to keep pace with novel attack methods, particularly where those methods are based on psychological manipulation rather than purely technical intrusion. Instruments such as the GDPR address data processing and data protection, but they do not directly regulate all forms of manipulation-based cybercrime.

Because offenders and victims are often located in different countries, cross-border crime creates additional obstacles for investigation and enforcement. In this context, Europol's coordinating function is particularly important (Europol, n.d.).

Artificial Intelligence, Social Engineering, and Their Legal Regulation

The emergence of artificial intelligence has opened an entirely new dimension in cybercrime, especially in the field of social engineering. Whereas traditional social engineering methods relied heavily on human creativity and manual data collection, AI enables the automation, scaling, and personalization of attacks. Consequently, manipulation becomes more effective and more difficult to detect.

[19] ENISA, 2023

Generative AI is particularly important because it can produce natural-language messages that appear authentic, imitate diverse communication styles, and interact with victims in real time. Deepfake technology adds a further layer of risk by allowing attackers to imitate real voices and faces. In this way, AI intensifies the psychological mechanisms of authority and trust that underpin many successful attacks[20].

Distinctive Features of AI-Generated Threats

The combination of AI and social engineering creates several new challenges. First, attacks become scalable, meaning that a single attacker can reach large numbers of targets. Second, attacks become adaptive, meaning that they can respond dynamically to victims' behaviour[21]. These characteristics reduce the likelihood of human recognition, increase the apparent credibility of attacks, and enable continuous learning throughout the attack process[22].

Regulatory Frameworks and Challenges

The linkage between AI and social engineering creates substantial challenges for legal regulation. Existing frameworks such as the GDPR focus mainly on data processing and data protection and were not designed specifically to address AI-based manipulation. The European Union has responded through the AI Act, which adopts a risk-based model and places particular emphasis on AI systems capable of manipulation or deception. Its purpose is to increase transparency, reduce the risk of abuse, and protect fundamental rights, although the rapid pace of technological change continues to challenge legislative responsiveness (European Parliament and Council, 2024).

International Cooperation and Future Regulation

Because social engineering and AI-generated threats are global in character, their management requires international cooperation. Organisations such as Europol play a crucial role in information-sharing and operational coordination. Looking ahead, greater emphasis will likely be placed on the ethical regulation of AI systems, the integration of technological and legal responses, and the protection of users against increasingly sophisticated forms of manipulation.

[20] C. Hadnagy
[21] Kahneman, 2011
[22] ENISA, 2023

Why Are People Manipulable in the Digital Environment?

The success of manipulation in digital environments cannot be explained solely by technological sophistication; it must be understood primarily in light of human cognition, decision-making, and social behaviour. Social engineering and its AI-enhanced variants are effective because they exploit basic psychological mechanisms that are integral to normal human functioning. Human beings are not defective when they trust familiar cues, respond emotionally, seek patterns, or cooperate with apparent authority figures. On the contrary, these are adaptive features of social life[23].

One of the most important reasons for manipulability is that people do not perform detailed rational analysis in every everyday decision. Instead, they often rely on heuristics. The speed, information overload, and constant stimulation of digital life amplify this tendency. Users confront large numbers of emails, notifications, messages, and requests every day, and they therefore frequently judge credibility on the basis of surface characteristics rather than deep verification. If a message appears official, urgent, visually familiar, or socially plausible, it is more likely to trigger automatic trust[24].

A second major factor is the role of emotion. Digital attacks often target fear, urgency, curiosity, anticipated reward, or respect for authority rather than reflective reasoning. When a person is told that an account will be suspended, a payment is in danger, a parcel has been delayed, or an extraordinary opportunity is available, the emotional reaction often precedes the verification process. This reduces critical distance and increases the likelihood of impulsive action.

Manipulability also has a fundamentally social dimension. Human interaction is ordinarily grounded in trust, cooperation, and norm-following. Social engineering exploits precisely this cooperative logic by imitating roles, relationships, and institutional scripts. In this sense, it is not merely informational deception but also social performance: the attacker plays a role, constructs a credible scenario, and thereby induces compliance[25].

The emergence of AI further deepens this vulnerability. AI tools can now produce grammatically correct, context-sensitive, personalized, and persuasive communications at scale. They can also imitate voices, faces, and conversational styles. As a result, the traditional cues by which users once distinguished legitimate from illegitimate communication are becoming less reliable, and the burden of detection increasingly falls on the individual's critical awareness (European Parliament and Council, 2024; ENISA, 2023).

Effective defence therefore cannot rely exclusively on technical controls. Although email filtering, authentication systems, access controls, and incident-response procedures remain essential, they cannot eliminate human susceptibility by

[23] Cialdini, 2021
[24] Kahneman, 2011
[25] Cialdini, 2021

themselves. A genuinely effective response must be layered and interdisciplinary, requiring digital literacy, critical thinking, regular awareness training, clear organisational protocols, and legal frameworks capable of addressing not only technical intrusion but also deception-based and AI-supported manipulation.

Conclusion

The study concludes that the technological advances associated with the Fourth Industrial Revolution have precipitated a substantive shift in the methodology of cybercrime. The effectiveness of online fraud now rests less upon the exploitation of technical vulnerabilities and more upon the deliberate manipulation of human cognitive processes and social dynamics - namely, the techniques of social engineering. The analysis demonstrates that perpetrators adeptly leverage evolutionarily adaptive mechanisms such as deference to authority, the norm of reciprocity and the principle of scarcity, alongside the fast, intuitive decisionmaking system articulated by Kahneman.

The advent of artificial intelligence and deepfake technologies has further amplified these threats, introducing a qualitatively new dimension to digital deception. Through automation and hyperpersonalisation, manipulation has become readily scalable, while visual and auditory falsification has grown increasingly difficult to discern. These developments extend beyond individual or economic harm: as instruments of hybrid warfare, they possess the capacity to erode public trust and generate societal disruption, thereby posing a direct and material challenge to national security.

Taken together, these factors underscore that addressing social engineering constitutes a complex and inherently interdisciplinary endeavour, requiring the sustained alignment of technological, legal and societal approaches.

References

1. Cialdini, R. B. (2021). Influence, New and Expanded: The Psychology of Persuasion. Harper Business.
2. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention), Budapest, 23.XI.2001.
3. ENISA. (2023). ENISA Threat Landscape 2023. European Union Agency for Cybersecurity.
4. Europol. (n.d.). European Cybercrime Centre (EC3).
5. European Parliament and Council. (2013). Directive 2013/40/EU on attacks against information systems.
6. European Parliament and Council. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation).

7. European Parliament and Council. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (AI Act).
8. Federal Reserve System. (2019). Synthetic Identity Fraud in the U.S. Payment System.
9. Federal Bureau of Investigation Internet Crime Complaint Center (IC3). (2018). 2017 Internet Crime Report.
10. Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking (2nd ed.). Wiley.
11. Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. Communications of the ACM, 50(10), 94–100.
12. Kahneman, D. (2011). Thinking, Fast and Slow. Farrar, Straus and Giroux.
13. Verizon. (2024). 2024 Data Breach Investigations Report.

Csaba Czakói[1]:

The shared responsibility space of technological transformation and work organization

Abstract:

In the twenty-first century, the relationship between work and health can be described less and less exclusively in the language of occupational safety rules and technical compliance. Working conditions are increasingly shaped by engineered systems: automated processes, sensor-saturated environments, remote supervision, data-driven control, and interconnected supply chains. Technological change moves together with transformations in work organization – flexible employment, project-based logic, outsourcing, hybrid work arrangements, and the redrawing of responsibility chains. This paper asks how the theme of "work and health in a changing world" can be interpreted from the perspective of engineering ethics. The central thesis is that engineering decisions do not only create tools; they also create work systems. Such systems define the form of exposures, the distribution of burdens, the handling of errors, and the room workers have for action and feedback. Consequently, occupational health protection cannot be reduced to a compliance logic (ISO, 2018). It is better understood as a responsibility practice in which due care, proportionate risk reduction, justifiable decision-making, and fair burden-sharing jointly determine the human conditions of work.

Keywords: engineering ethics; occupational health; technological change; work organization; responsibility

Introduction

The theme of "work and health" in a changing world is more than a narrow policy question: it is one of the basic problems of modern technological society. Work simultaneously means production, service, and social cooperation, while also producing everyday exposures: physical hazards, sustained loads, and cognitive and psychological pressure. Health in this context is not merely the absence of accidents. Health is the sustainability of working: to what extent a work system can operate without gradually depleting bodily and mental resources.

[1] University of Pécs, Faculty of Culture, Education and Regional Development, e-mail: czakoics@gmail.com

The changing world is often described through technological slogans: automation, industrial digitalization, smart devices, data, predictive maintenance. These phenomena are indeed influential. Yet technology rarely changes work on its own; its effects are realized through work organization. New tools bring new time regimes, new competence expectations, new forms of control, and new distributions of responsibility. Change is therefore neither exclusively technical nor exclusively organizational: the two are intertwined. The present paper treats this intertwinement as the primary object of engineering-ethical analysis. (Beck, 1992).

In this context, engineering ethics is not merely "professional ethics." It examines the normative conditions of technical decisions. An engineer does not only solve a task; they create a solution that structures work: what must be monitored, when intervention is required, what counts as abnormality, how much slack remains in time and resources, and what kinds of errors the system is prepared to handle. These decisions are partly invisible in everyday practice, yet they directly influence whether work becomes health-supporting or health-eroding (Reason, 1997; Leveson, 2011).

Methods

Two proportions define the paper's emphasis. The analysis of change focuses approximately two-thirds on technological aspects and one-third on work-organizational aspects, because technological development typically first reshapes the materiality of work processes and, through this, forms organizational decisions. At the same time, organizational logic feeds back into technology: cost and deadline pressure, outsourcing, and project-based operation often call forth technical solutions that hide or delay certain burdens. For this reason, the two dimensions must be considered together.

The method is conceptual and normative: it makes explicit the assumptions embedded in engineering decisions and examines the minimal requirements under which a work system can be considered health-protective. The analysis is not restricted to a single industry; examples remain intentionally general so that the conclusions can be applied across multiple work environments (Wilson & Sharples, 2015).

Results

1. Conceptual framework: work system, health, responsibility

Work in practice is broader than a task: it is a work system. A work system is the combination of the task, tools, environment, time regime, feedback, and decision rights. Engineering design appears at multiple points in the work system: workplace layout, ergonomics, human–machine interfaces, process and maintenance logic, steps of error handling, and the configuration of automated alarms and interlocks.

The work system is thus already a technical and organizational structure, even if everyday language does not always make this visible.

The concept of the work system is useful because it shows that health at work is not exclusively a matter of individual lifestyle. The work system shapes the rhythm of the body and the rhythm of attention. It determines whether there is time to notice errors, whether one can stop and reassess, and whether there are channels for feeding back experience. It also determines whether the person stands at the center of the system, or whether they are forced to "chase" the process from its margins.

The concept of health in the context of work has multiple layers. There is acute health risk, which appears as accidents or immediate harm. There is chronic risk, which develops over time through cumulative burdens. There is also psychological and psychosocial risk: sustained stress, overload, role conflict, loss of control, and uncertainty. A characteristic of the changing world is that some classical physical risks may decline while cognitive and psychosocial burdens may increase. An adequate account of occupational health must therefore consider all three layers (Karasek & Theorell, 1990).

It is useful to understand responsibility as a normative relation between agents, decisions, and consequences. Responsibility is not generated at a single point. First, there is causal responsibility: who caused the harm. Second, there is role responsibility: whose task it was to prevent or detect the risk. Third, there is institutional responsibility: what rules, incentives, and resource conditions made a harmful outcome possible or likely. In work systems it is common for these dimensions to drift apart. At the moment of harm, the person closest to the consequence often has the least room for manoeuvre. A key task of engineering-ethical analysis is to make this distortion visible and to propose more balanced arrangements of responsibility relations (Reason, 1997).

The relationship between responsibility and power is of special significance. In the changing world, the decision space of technological systems often moves away from the site. Parameters are set centrally, algorithms set work rhythm, predictive models schedule maintenance. In such cases, responsibility often remains where power no longer does. From the perspective of occupational health, this means that design and management must assume the consequences of their decisions and cannot shift the "handling" of risk onto executors.

2. Technological changes: the changing materiality of work

2.1 Automation and the burden of exception handling

Automation is often presented as replacing dangerous, monotonous, and heavy work. In many areas this effect is real. At the level of the work system, however, automation typically rearranges the structure of the task: routine becomes supervision, continuous manual intervention becomes exception handling. The system runs

by itself in “normal” conditions; the human becomes central in abnormalities. This role shift has significant health consequences.

Supervisory work often requires long periods of readiness while rarely providing feedback on performance. Sustaining attention can cause monotony and fatigue, yet in the critical moment the work demands immediate, high-stakes decisions. Cognitive load here arises mainly from abrupt switching rather than continuous activity: a quiet state suddenly becomes a critical state. If system signals are ambiguous, or if multiple alarms arrive at once, the probability of error increases. Design responsibility therefore includes ensuring that exception handling does not remain a space of “worker improvisation.” It requires clear signals, prioritized alarms, understandable intervention steps, and opportunities for practice (Bainbridge, 1983).

A further consequence of supervision is that the worker can easily become the system’s last line of defense. In everyday operation, automation carries the load; in anomalies, responsibility suddenly falls to the on-site or remote operator. This concentration can cause psychological burden, especially when decision rights are not proportional to responsibility. In this situation, occupational health is inseparable from decision support: good decision support protects health by reducing interpretive uncertainty and unnecessary alarm noise (Parasuraman & Riley, 1997).

A less discussed consequence of automation is the rearrangement of competence. When the system performs many operations automatically, manual skills and on-site routines may slowly erode. This becomes critical in extraordinary situations when the system hands the task back to the human. For health, this creates a double burden: high vigilance must be sustained, while genuine opportunities to practice rare but critical skills are limited. Design responsibility therefore includes embedding training and simulation: the system should not only run; it should be teachable and learnable (Parasuraman, Sheridan, & Wickens, 2000).

2.2 Sensors, data, and the limits of perception

Sensor-rich environments and real-time data collection promise new possibilities: early warnings, condition-based maintenance, risk prediction. In engineering practice, these often appear as the promise of prevention. In reality, measurement provides information and simultaneously creates a way of seeing. What can be measured is more easily treated as a problem; what is not measured easily recedes into the background.

This is especially sensitive for occupational health. Some physical exposures are well measurable, so systems can enforce threshold compliance. Other burdens are harder to measure: fatigue, stress, overload, attentional errors, or micro-injuries often appear only later in indicators. If a work system builds exclusively on easily measurable dimensions, “invisible” burdens shift onto workers. This is a system effect rather than ill will: measurement architecture defines the focus of attention. An engineering-ethical requirement is therefore that the system should not treat

hard-to-measure burdens as irrelevant. Design must also create feedback loops that convey experience alongside numbers: reporting channels, on-site feedback, and regular interpretive discussions (Wilson & Sharples, 2015).

Another practical problem of sensor systems is false alarms and alarm overload. If the system signals too much, attention fatigues and signal credibility erodes; if it signals too little, risk remains hidden. Finding the right setting is not only technical fine-tuning but also an occupational health issue: the rhythm and quality of alarms directly influence stress levels and decision burden.

2.3 Data-driven control and the normative effects of performance measurement

One consequence of digital control is the visibility of performance. Work processes can be tracked, cycle times measured, error rates compared. This can help organizations learn and improve. At the same time, performance measurement has a normative effect: it defines what counts as "good work." If the system rewards only speed or output, rest, careful checking, and risk management may become marginal. If it demands only faultlessness, silence and data massaging may emerge. From an occupational health perspective, both tendencies are harmful: either overload rises, or problems surface later at higher cost (Moore & Robinson, 2016).

In the changing world, performance evaluation increasingly relies on digital logs and automated reports rather than personal managerial observation. The worker may experience that the rhythm of work is set by "the system." This sense of control is an important health dimension: if workers do not understand what is measured and why, and cannot contest distortions, psychosocial strain increases (Karasek & Theorell, 1990). The engineering-ethical question is therefore also the extent to which measurement is explainable and debatable. A good measurement system does not merely produce numbers; it makes clear what counts as deviation and why.

Engineering design is present here as well: software logic, thresholds, exceptions, rankings are all designed elements. The ethical stake is that workers' health and dignity should not become a hidden externality of efficiency. The point is not to reject measurement but to require forms of measurement in which sustainable work remains part of the success criteria (Zuboff, 2019).

2.4 Remote operation and the distance of responsibility

Remote operation and remote supervision are among the most visible consequences of technological change. Reducing on-site exposure can itself be a health gain. Yet remote operation creates new kinds of vulnerability. Decision makers become distant from the experiential reality of the situation. The data visible on a screen are selected, and much on-site context is missing: sounds, vibrations, and the felt "strangeness" of an environment often do not pass through the digital channel.

This distance increases decision risk and can also cause psychological burden. A remote operator may feel the weight of responsibility while execution is shifted to on-site teams. If communication is unclear, or if decision rights are not well defined,

conflicts arise and working conditions deteriorate. Engineering ethics therefore demands that designing remote systems is not merely about data transmission; it is equally about designing responsibility and communication relations.

A further form is moral distance: when decision makers do not directly see what burden their decisions impose on those on the site. Such distance increases the risk that the real difficulties of work become invisible. Protection strengthens when remote decisions are paired with feedback: on-site reports, joint analyses, and protocols that support rather than punish the right to stop work (Dekker, 2012).

2.5 Human–machine cooperation, ergonomics, and sustainable use

One promising area of technological change is improving human–machine cooperation. Collaborative robots, lifting aids, and exoskeletons may reduce physical load. Such solutions become health gains only if conditions of introduction are also adequate. Use ergonomics, training, maintenance, fault signaling, and systematic remeasurement all matter. If a tool is uncomfortable, slows work down, or appears as an obstacle, workers may bypass it. Then exposure returns and the organization may blame workers for a situation actually created by system design.

Sustainable use is also an engineering-ethical issue. Design responsibility extends beyond the prototype. Technology that works well only under ideal conditions can easily cause harm in real work systems. In a changing world, technological interventions should not be quick "fixes"; they should function as elements that evolve with the work system – through feedback, refinement, and the integration of workers' experience (Wilson & Sharples, 2015).

2.6 Maintenance, life cycle, and "hidden work"

The impact of technological systems on health often becomes visible during operation and maintenance. Maintenance frequently creates situations where protections must be temporarily removed, covers opened, or hazardous spaces entered. Maintenance is typically performed under time pressure because downtime is costly. Occupational health therefore critically depends on how "maintainable" a system is: accessibility, well-designed lockout/check points, and clear conditions for safe states.

Digitalization can bring gains here as well: condition-based maintenance, prediction, documented intervention steps. Yet it can also introduce new burdens. If maintenance is optimized too aggressively, work is forced into narrow windows and room for manoeuvre shrinks. If documentation is complex, on-site action collides with administrative expectations. Design responsibility here means not treating maintenance as secondary: maintainability and safe intervention are basic design requirements.

2.7 Technological transitions: implementation, change management, learning

In a changing world, some risks arise in transitions rather than in "stable operation." Introducing a new system, software updates, configuration changes, new

suppliers, new procedures – these are situations where established routines break. In transition periods, error probability rises because workers are still learning the new logic and system behavior may be less predictable. Occupational health is also affected: overtime, rapid training, and continuous "live" experimentation can be exhausting.

Engineering-ethical responsibility in transitions is to treat implementation not merely as a technical project. Implementation reorganizes the work system; therefore training, pilot runs, feedback, and learning from error are essential. The quality of change management is directly linked to occupational health because poorly managed transitions leave lasting stress and distrust.

2.8 Digital documentation and administrative burden

Digitalization often increases the burden of documentation alongside making work "visible." Parts of work count as completed only if recorded in the system: checklists, photo documentation, electronic logs, signatures, confirmations. Documentation is not pointless; in many cases it enables learning and clarifying responsibility. Problems arise when documentation works against the rhythm of work: it interrupts concentration, delays intervention, or forces parallel administration.

For occupational health, this can create a double burden. Cognitive load rises because the worker becomes both executor and "data-entry" agent. Frustration rises if the system enforces formal steps detached from on-site realities. Engineering-ethical responsibility is not to deny administration but to find a workable ratio: documentation should serve safety and health rather than become a hidden risk amplifier.

A subtle dilemma is that documentation often does not count as "real work" in performance evaluation. If output or cycle time is rewarded, documentation time looks like "loss," and workers may compensate at the expense of their health. Sustainable work systems therefore need to recognize documentation time and significance in design: careful work takes time.

3. Organizational changes: time regimes, outsourcing, responsibility gaps

3.1 Flexibility and time regimes: new rhythms of burden

Work organization changes together with technology. Flexible employment forms, project-based operation, and outsourcing are often tools of competitiveness. From a health-protection perspective, however, they frequently mean the disruption of time regimes and stability. Rotating shifts, on-call burden, and shortened rest periods increase fatigue risk. Fatigue is not merely a wellbeing issue; it directly worsens attention, reaction time, and decision quality (Karasek & Theorell, 1990).

Digital systems often make work "visible" and simultaneously densify it. Task allocation is faster, scheduling tighter, delays instantly flagged. For organizations this is efficiency; for workers it can become constant urgency. Occupational health

here is a matter of rhythm: is there space for recovery, is there real rest, and can the system operate quietly without continuous intervention demands?

3.2 Outsourcing and responsibility gaps

Outsourcing and subcontractor chains can be particularly problematic from a responsibility perspective. The technical system may operate as one, but responsibility chains fragment. Burdens can concentrate where protection is weakest: short training, incomplete information, precarious employment, strong deadline pressure. The ethical question is not whether outsourcing is "good or bad," but how health-protective conditions remain consistent across the chain.

Project logic often encourages splitting work into phases and tying responsibility to contract points. Health risks, however, do not always align with these points. Interfaces - handoffs between teams - are often especially hazardous because context is partly lost. Engineering design matters here too: documentation, handover protocols, markings, and shared check points can reduce burdens arising from misunderstanding (Leveson, 2011).

3.3 Hybrid work and digital exposures

Hybrid work and remote work have become durable in many areas. Physical exposures may decline, while sedentary work, screen time, constant online availability, and blurred work–life boundaries create new burdens. Technology here is both tool and medium. Platforms, communication channels, and workflow systems shape work rhythm and interruptions.

Occupational health in such settings is partly a design issue: notification logic, priority handling, and built-in "quiet time" within schedules. From an engineering-ethical perspective, systems should protect human time: technological possibility (constant reachability) should not become a norm (constant expectation).

3.4 Training, knowledge, and generational change

In a changing world, tools change quickly and staff turnover may rise. This makes knowledge management an occupational health issue. Tacit experience is often a protective factor: workers recognize from subtle cues that "something is off." If knowledge transfer fails, uncertainty and stress increase, and errors rise. Technical systems can help (better documentation, visual support, simulation), but implementation remains decisive. Technology does not automatically replace communal learning.

4. Engineering-ethical orientation points for protecting occupational health

To grasp the work–health relationship in engineering-ethical terms, we need concepts that are not slogans yet still provide orientation. Four anchors are particularly important: care, proportionality, justifiability, and fairness.

4.1 Care: systems that anticipate error

Care in design means that the system anticipates human limitations. Workers can err, tire, have divided attention, and lack full information. A careful system is therefore error-aware: it provides understandable signals, uses interlocks that prevent real danger, and builds slack so that situations remain manageable (Reason, 1997).

A related requirement is that the system should not force workers into constant "creative workarounds". If everyday work continuously requires bypassing rules, then the rule system is flawed and health burden lands on workers. Design responsibility is then to treat real work as the measure: rules should be followable in sober practice.

4.2 Proportionality: effective risk reduction and real protection

Proportionality is a realistic principle of risk reduction. Occupational health protection is often a space of trade-offs because resources are limited. Proportionality, however, is not arbitrary concession. There are effective and less effective forms of risk reduction. Purely administrative measures are rarely sufficient on their own. Durable reduction depends more on process redesign, elimination of hazardous steps, engineered safeguards, and appropriate organizational solutions (Leveson, 2011).

The ethical side of proportionality is that protection cannot be merely symbolic. If risk is high, protection must be strong; if risk is rare but severe, preparedness and preventive steps carry particular weight. Engineering responsibility is to avoid stopping at the "most convenient" level when risk and consequence justify stronger interventions.

4.3 Justifiability: transparent decisions and traceable trade-offs

Justifiability concerns the quality of decision-making. Technical and organizational decisions rarely occur under full certainty. Therefore a decision has not only an outcome but also a rationale. Justifiability means reasons are transparent, trade-offs can be stated, and experiential knowledge of work is built into deliberation.

With the spread of digital systems, justifiability takes a new form. Algorithmic or optimization decisions are often treated as "objective." For occupational health, it is not enough that the system calculates; users must be able to understand what and why it recommends. If decision logic is inaccessible, workers feel exposed and responsibility practice weakens. Engineering ethics therefore asks that systems not only function but be explainable at least at the level required for correct intervention (Parasuraman et al., 2000).

4.4 Fairness: burden-sharing and vulnerability

Fairness concerns the distribution of burdens and protections. In the changing world, those bearing the greatest risk often have the fewest resources to protect themselves: subcontractors, temporary workers, people in vulnerable positions. En-

gineering ethics asks on whose burden the stability of the system is built. Fairness is a precondition of sustainable work. If risks are persistently shifted to a narrow group, organizational functioning and social legitimacy are also harmed.

A practical requirement of fairness is that risk assessment should not assume only an "average worker." Age, physical characteristics, training, language competence, and employment stability all influence vulnerability. Responsible design does not optimize for an imagined ideal user; it can accommodate the heterogeneity of real work (Wilson & Sharples, 2015).

4.5 Decision points: where occupational health is "produced" in technical systems

From a practical standpoint, occupational health does not depend on a single major decision but on many smaller design choices. One such point is whether a hazardous operation can be eliminated at the beginning of a process or only "covered" at the end with PPE and procedures. Another is accessibility: can maintenance be performed in comfortable posture, with good lighting and clearly marked lockout positions, or does the design create forced postures and time pressure? Such choices, which may look like technical details, draw long-term occupational health trajectories: either they reduce the accumulation of burdens or they quietly build them into everyday practice.

In a changing world, interface design becomes another decision point. Interfaces support health when they do not overload attention: signals are prioritized, language consistent, critical information not lost in noise. Poor interfaces do not only lead to errors; they also cause chronic stress because they keep operators in constant uncertainty. Here occupational health converges with human factors engineering: systems should cooperate with users rather than expect users to compensate for system deficiencies.

Consider a brief example. In warehousing or manufacturing, digital task allocation and scanning can increase accuracy, while narrowing workers' room for manoeuvre. If performance is evaluated minute by minute, workers tend to skip micro-breaks, speed up movements, and pay less attention to bodily signals. The result may not be immediate accidents but gradual strain, musculoskeletal problems, and exhaustion. The engineering-ethical question is whether system design treats strain reduction as a legitimate goal and is willing to constrain efficiency within limits that protect sustainability (Moore & Robinson, 2016).

4.6 Professional integrity and speaking up: engineering responsibility under organizational pressure

One constant companion of technological and organizational change is performance pressure. Fast implementation, tight budgets, and continuous operation needs easily create situations where risks appear "temporarily" acceptable. For occupational health, "temporary" solutions often become permanent because the system adapts to them. Engineering responsibility in such environments is not only the correctness of

calculations and plans. It includes professional integrity: being able to state when a solution substantially increases workers' burden or when implementation conditions are not mature.

Speaking up and signaling are not only questions of personal courage; they have institutional conditions. How does an organization handle bad news? How does it respond to stop-work? How well does it protect those who report risk? Engineering-ethical analysis highlights that responsibility practice cannot be separated from organizational environment. If an organization punishes reporting, risk stays hidden and burden appears in workers' health. If reporting is treated as a learning opportunity, occupational health protection becomes part of everyday operation (Dekker, 2012).

In a changing world, it is crucial that engineering responsibility does not shrink to "meeting the specification". Specifications often fail to see fine details of real work. Sound engineering judgment connects system logic with on-site experience. Without this link, technological development easily creates work systems that are efficient on paper but health-eroding in practice (Reason, 1997).

4.7 Risk and uncertainty: what does "acceptable" mean in occupational health?

A difficulty of protecting occupational health is that some burdens cannot be described with precise probabilities. Accident risk can often be quantified, whereas chronic burdens and psychosocial effects are more uncertain: they develop slowly, arise from multiple factors, and become visible only later. In a changing world, such uncertainty may increase because the effects of new technologies and time regimes are not always known in detail.

Engineering-ethical responsibility under uncertainty is precautionary. It does not require perfect prediction. It requires taking possible harms seriously and being especially cautious where consequences are severe or long-lasting. In occupational health, this means that "no complaints at the moment" is not enough. Systems must recognize early signals and intervene before burdens turn into widespread health deterioration.

Managing uncertainty is also a matter of justification. A decision is responsible when its reasons are clear, risk-reduction steps traceable, and the organization commits to revising technology and work organization if needed. One form of responsibility in a changing world is corrigibility: the system does not treat its settings as final; it can learn from the lived experience of work (Hollnagel, Woods, & Leveson, 2006).

Summary

Work and health in a changing world is a complex issue in which technological and organizational decisions continuously interact. Technological transformation can reduce classical hazards while also creating new burdens and vulnerabilities.

Organizational changes can create flexibility while often disrupting stability and opening responsibility gaps.

Engineering ethics can contribute to addressing the problem of work and health by linking these two dimensions. The central claim of this paper is that engineering decisions create work systems. Occupational health protection is therefore not an after-the-fact patch; it is a design issue.

Care, proportionality, justifiability, and fairness are anchors that help tie technological development to the strengthening of human conditions.

Finally, it is worth emphasizing that an engineering-ethical treatment of occupational health is not merely an industry-specific matter. Technical systems are now present in services, transportation, health care, and information work as well. For this reason, the stakes of "work and health" extend further: engineering decisions indirectly shape societal patterns of health.

Responsibility practice becomes credible when design, operation, and organizational leadership find a shared language. They do not shift burdens onto one another; they organize decisions around the same goal – safe and sustainable work.

A changing world does not reduce the need for responsibility; it expands it. The more complex the system, the more important it is for the health of work to appear as an explicit goal in design and organizational decisions.

The ultimate stake of the engineering-ethical approach is that technological rationality should not become a closed goal system. The health of work is not a side effect; it is a qualitative condition of operation. If this insight is embedded in design and operation, a changing world can make work more humane, more sustainable, and healthier.

References

1. Bainbridge, L. (1983). Ironies of automation. *Automatica, 19*(6), 775–779.
2. Beck, U. (1992). *Risk society: Towards a new modernity*. Sage.
3. Dekker, S. (2012). *Just culture: Balancing safety and accountability*. Ashgate.
4. Hollnagel, E., Woods, D. D., & Leveson, N. (Eds.). (2006). *Resilience engineering: Concepts and precepts*. Ashgate.
5. ISO. (2018). *ISO 45001:2018 Occupational health and safety management systems – Requirements with guidance for use*. International Organization for Standardization.
6. Karasek, R., & Theorell, T. (1990). *Healthy work: Stress, productivity, and the reconstruction of working life*. Basic Books.
7. Leveson, N. (2011). *Engineering a safer world: Systems thinking applied to safety*. MIT Press.
8. Moore, P. V., & Robinson, A. (2016). The quantified self: What counts in the neoliberal workplace. *New Media & Society, 18*(11), 2774–2792.

9. Parasuraman, R., & Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. *Human Factors, 39*(2), 230–253.
10. Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans, 30*(3), 286–297.
11. Reason, J. (1997). *Managing the risks of organizational accidents*. Ashgate.
12. Wilson, J. R., & Sharples, S. (Eds.). (2015). *Evaluation of human work* (4th ed.). CRC Press.
13. Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.

Marcell Szilovics[1]:

The role of green taxes in the implementation of a sustainable economy and problems of their practical application

Abstract:

In my work, I reviewed the legislative and taxation processes related to environmental protection and analysed some frequently used tools. In my work, I briefly presented the historical stages of climate protection. I then analysed the functioning and effectiveness of various legal instruments, ranging from discretionary regulatory elements to legal prohibitions. I observed that explicitly prohibitive norms are the most effective weapons of environmental protection because, if they are based on thorough impact studies, precisely formulated rules, and expert work, they can significantly reduce the environmental impact caused by societies. I briefly introduce greenwashing and also mention a couple of truly unethical greenwashing tactics used by companies. In the main part of my work, I examined the functioning of green taxes and their actual environmental impact. I also considered what makes a tax green, despite the fact that there are several definitions of green taxes accepted by experts. I also compared international and domestic legislation and found that countries apply them in different forms and to different degrees, with the result that national green taxes and tax systems are not comparable. The imposition of green taxes is not always the appropriate response to the problem at hand, so other options need to be thoroughly explored. When applying green taxes, special attention should be paid to consumption flexibility and the differentiated treatment of basic consumer goods. The result of my research was that in most cases, significant environmental results can be achieved when green taxes are introduced in conjunction with other environmental policy measures. Green taxes can be effective in that they enable the state to steer consumers and economic actors towards the most sustainable solutions. In my work, I conclude that taxation is always a cultural phenomenon, which is why green taxes can only be effective in a social environment that is consciously committed to environmental protection. Poorly applied environmental taxes merely increase budget revenues and place an additional burden on taxpayers, undermining tax morale and failing to support the cause of environmental protection.

Keywords: Greenwashing, sustainability, green taxes, climat probleam, recycling

[1] University of Pécs, Faculty of Law, fifth-year full-time law student

Introduction

The main objective of my work was to examine the legal instruments to combat climate change in our immediate and wider environment, from voluntary compliance to soft law elements and the role of green taxes. In the first part of my thesis, I present the historical background of the fight against sustainability, define the basic concepts involved, analyse the effectiveness of voluntary compliance and soft law instruments and the phenomenon of greenwashing, and then examine the types of green taxes introduced to promote sustainability, I undertook this research because I believe that one of the big questions of our time is whether legislators, using the tools of the tax system , can respond to the phenomenon of pollution and develop effective tools for climate protection.

By the beginning of the 21st century, most politicians and ordinary people have understood that delaying environmental action is dangerous for the planet because we are running out of the raw materials[2] needed to keep society functioning. At the end of the 2010s, the world's population resource demand exceeded the Earth's biocapacity by 70 percent[3], and according to Global Footprint Network, human consumption exceeded the level that the Earth can replenish in a year on 1 August this year. It is astonishing that in 1970 this point was only reached on 23 December. Meanwhile, each inhabitant of the planet leaves behind an average of 560 kg of rubbish per year[4], while the earth's population continues to grow at a dynamic rate. Faced with the effects of this destruction, more and more people are recognising that climate change and the drastic loss of biodiversity are largely caused by humanity's exploitative lifestyles and economically unsustainable practices. Business actors are aware that 20 percent of the types of raw materials currently used will be exhausted within the next 50 years and nearly 35 percent within 100 years, while most of them are not reused[5].

As a law student, I also believe it is important for science actors to identify harmful phenomena such as greenwashing, which is carried out unethically by some companies for profit. I believe that it is up to our generation to draw attention to these harmful business phenomena. Despite the fact that politicians and economists have introduced the concepts of circular economy and eco-production and sustainability into public discourse and legal norms, and that natural scientists are producing increasingly efficient products, we forget that taxation can be one of the most effective tools for influencing human behaviour. Therefore, it is good news in the fight for environmental protection that green objectives in taxation systems have been around for decades and in my work I will try to explore the legal options that can achieve significant energy and material savings through taxation with little

[2] Marnitz István: Kifogytunk a nyersanyagokból Népszava 2021. 12. 20.

[3] Global Footprint Network, 2021. idézi Bögöthy Zoltán-Hausmann Róbert: Új, zöld és fenntartható adórendszer 541. MNB kutatás 17. fejezet

[4] PWC szakmai anyag 2018 6-oldalán idézi az OECD 2012-es adatát.

[5] PWC Szakmai anyag 2018. 9.

financial input, and I will present the successes and failures of the financial instruments currently in use.

On the emergence of the idea of environmental protection

Until the 19th century, the question of the existence of a sustainable or environmentally friendly economy and society only arose in communities where relatively large numbers of people settled in small areas, such as in ancient Egypt, Mesopotamia, India and some parts of China. At the end of antiquity, cities of several hundred thousand people were established on the Italian peninsula, in Alexandria in North Africa and in the Mohenjo Daro in India, where the huge population density caused social problems and required regulation to deal with the accumulated waste. Such a situation arose in imperial Rome, where the lives of more than a million inhabitants were governed by environmental, fire and waste management regulations. In the silver mines of Hispania, the environment was heavily polluted and taxes were so high that they were levied on the population of the region. In the 3rd century BC, they imposed heavy taxes on agricultural farms, causing many thousands to abandon[6] production. Epidemics, fires, famines, mass poisonings forced the leaders of the overcrowded cities of the medieval and early modern world to create environmental and coexistence regulations on water use, burial, waste management, crafts and trades in order to create a healthier human environment. This legislative process also appeared in our country: from the 15th century, Buda, the centre of the Hungarian kingdom, and several of our larger towns had ordinances on waste disposal, and in the late 18th century Joseph II, an early environmentalist, ordered the use of reusable coffins to protect forests. However, even in the 19th century, 95-98% of the country's population lived and worked in rural agrarian communities, where they lived their lives sustainably without polluting the environment. Human life and the living environment were radically transformed by the industrial revolution in Western Europe and North America, where humanity became familiar with the phenomenon of waste pollution, highly toxic smoke, water and soil pollution. From the second half of the century onwards, the world economy in a growing number of countries from the United States of America, France, Germany and then Russia and the Austro-Hungarian Empire was a one-way street, taking resources from nature, producing products to be consumed, and throwing away the surplus to create mountains of waste. As the Nobel Prize-winning chemist Crutzen put it, "man became a shaper of nature" and the age of humanity dawned as the exploitation of the planet's resources and the process of colonisation accelerated in the mid-20th century.[7] Fortunately, the increased exploitation of our land went hand in hand with the strengthening of the idea of environmental protection and, at the request of the Club of Rome, the Meadows report entitled 'Limits to Growth' was produced in

[6] Kiss József: Biztos jelek, amelyek a birodalmunk bukásához vezetnek, G7.hu, Élet Világ 2023. 12. 29. 3.
[7] Crutzen-Stoemer-Steffen: The Future of Nature, Yale University Press, 2000.

1972, in which the idea of the finite nature of environmental resources was formulated. Subsequently, the first rules specifically designed to protect the environment were drawn up in the United States under President Nixon, and the UN and the EU also launched legislative processes. The wider public became aware of the problem when the first world-scale global climate panic broke out in 2003, with a heatwave causing many deaths in many countries, and in the following years record drought and crop failure hit the Middle East and Africa, triggering the first major wave of migration.

Some basic environmental concepts

As far as the use of environmental concepts is concerned, we can identify a few universally recognised and used definitions: sustainability, circular economy and green or eco-taxes, which I have used frequently in my work. In science and international law, the concept of *sustainability* was the first to appear, referring to the conservation of community and natural values. Sustainable development is the process of meeting the needs of the present society and economy without compromising the future generations to meet their own needs According to Pearce[8] and colleagues, sustainable development means that the level of human well-being per capita does not change over time. A completely different approach to sustainability is the concept of *a circular economy,* in which the current economic systems are transformed to focus on waste management rather than on the continuous improvement of production. At the heart of this approach is the economic and business objective that, in an optimally managed circular economy, waste is virtually eliminated, because what cannot safely decompose in the environment is used by economic actors. The point is that waste should not be generated, but if it is, it should be recyclable or reprocessable and only as a last resort should it be landfilled or incinerated. In achieving this, waste management, the use of materials in production, the consumption footprint, recycling and innovation are key challenges. In a circular economy, the products of today provide the raw materials of tomorrow, where the design, production and consumption of products are rethought, opening up new, untapped markets for entrepreneurs[9] . The model is not yet perfect, with only 9.1 percent of the world's materials being recycled in 2018 and 8.6 percent in 2022. Unfortunately, this rate has been steadily declining in our country since 2012.[10]

A larger scale change could be brought about by the introduction of a product charge and plastic bottle redemption in European countries. The undoubted benefits of a circular economy would be to save materials and energy, reduce the price of raw materials and improve the predictability of supply, create new jobs, stimulate

[8] Brundland Report ENSZ, 1987., illetve hasonlóan fogalmaz Pearce és Warford 1993-ban. Megjelent A fenntarthatóság és a gazdasági fejlődés megjelenése a versenyképességben 2020. 09 Leadership Kk. Biatorbágy 14-20

[9] Ha a kör bezárul- a körforgásos gazdaság jelentősége és lehetőségei, PWC 2018. Szakmai tájékoztató 4.

[10] Kákos Anna: Sosem lesz körforgásos a gazdaság, amíg a jogszabályok nem kényszerítik ki, hvg.hu 2022. 06.

innovation, increase the international competitiveness of the economy and achieve a sustainable economy. The third concept that I will introduce is the definition of *green or eco-taxes,* where scientists and politicians emphasise, with or without reason, that their imposition is primarily driven by their environmental impact, i.e. their application either directly improves the state of the environment or the revenues from these sources indirectly support the sustainable economy and protect the earth's climate.

The entirely voluntary phase of environmental protection and the role of positive incentives

When the idea of environmental protection first emerged in the 20th century, volunteering was at the heart of action plans, because for decades the leading politicians of the time naively believed that environmental protection could be achieved through education, education and volunteering, without any state coercion. This is why the building of the world's environmental protection institutions began relatively late, some 70 years ago, when the European Community had already mentioned environmental protection in its founding treaty of 1957, but the founding politicians had not yet set goals, expectations and rules. A few decades later, the need to develop and improve environmental protection programmes was first formulated at the 1972 UN conference in Stockholm and our natural environment was defined as the common heritage of mankind. All studies have shown that the level of voluntary compliance and voluntary protection of the environment is determined by the economic, wealth and cultural level of a community. According to a study conducted in 2022, which surveyed 350 companies worldwide on the basis of their sustainability objectives and practices, the Nordic countries and small Asian tigers with high per capita income and education and small average wealth gaps between social strata performed best. In contrast, Romanian companies scored only 43 out of a possible 100 points in this survey, placing Romania at the bottom of the world ranking according to the Institute for Environmental Sustainability[11] .There are some good initiatives, however, fortunately governments have launched a number of environmental programmes without legal constraints, from subsidies for solar panels, to selective waste collection, to the return of plastic bottles. For-profit companies have also been involved in good and dispositive initiatives, such as the Rosmann department store chain, which has eliminated plastic shopping cards, the Hungarian-founded Biotech USA, which promotes various forms of social responsibility, and MOL, which is at the forefront of recycling, collecting waste oil and hazardous household waste.[12] Even without state support, electric cars are still popular in Norway, where they have the highest share of ownership in the world. The number of e-cars will exceed the number of petrol cars in 2024, according to the

[11] Nem érdekli a román cégeket a környezetvédelem Pormolió.hu 2023. 02. 03.
[12] Zsuppán András: A Szajnát igenis megtísztították, Válasz online.hu, 2024. 08. 15

Norwegian Road Association[13]. An example of *efficient and well-used* public support is the installation of solar panels, which has been supported by the EU and the Hungarian government in the past. The EU has made the installation of solar panels mandatory for all new real estate investments in 2024, for non-residential and public buildings from 2027 and for all new residential buildings from 2030, which will also be mandatory in Hungary[14]. A similarly successful climate protection project seems to be the mandatory glass redemption scheme, which reflects the circular economy approach. Several EU Member States have introduced it independently. Data for the first half of the year show that in Romania the collection rate for selective bottles has increased from 13% to 80% by August[15]. The problem is that national procedures differ and each national law has different requirements. There has also been a lot of controversy about the mandatory use of fixed caps. Packaging expert Markus Prem of the University of Applied Sciences in Kempten says that this measure is not logical because, in his opinion, the amount of caps that end up in the sea, rivers and lakes is very small and therefore the environmental reference is not justified. EU regulation has forced the industry to invest billions in new machinery, for example. The German Beverage Wholesalers' Association believes that the costs of converting the systems are in the order of millions of euros, Der Standard reports. According to the German Food Industry Association, the significant costs are in the region of €181,000 per filling line, with the new cap solutions costing around 0.2 cents more per filling line, according to Peter Feller. The association's deputy CEO added that Europe and America account for a small share of plastics washed into the sea, with the vast majority coming from Asia, according to economix.hu[16]. Despite the controversy surrounding glass recycling, MOL, the operator of Hungary's MOHU system, is extremely optimistic and plans to recycle most of the 3.5 billion bottles, jars and cans generated in Hungary each year. Their target is to reach 90% within a few years, which would require 7-7.5 million returns per day, and the company plans to have a collection rate of 25% by 2025 and 30% by 2030.[17]

Options for legal regulation

When the legislators of the nation states were first confronted with the problem of environmental damage, local pollution of living water, soil or air in the 19th and 20th centuries, they relatively quickly recognised the causal links and sought to identify the cause of the damage, the individual companies. To deal with this clear legal situation, the principle of "polluter pays" was developed in civil and criminal law and the various state environmental or agricultural and wildlife protection agencies,

[13] Zádori Bence: Elérte Norvégia azt, ami máshol még csak álom, Economx.hu, 2024. 09. 19.
[14] Hatályba lépett: kötelezővé vált a napelemek telepítése az Unióban 2024. 08. 22.
[15] Lemostuk a szégyent-Románia lsztább, Maszol.ro 2024. 09. 24.
[16] Csomor Zsolt: Értelmetlen találmány a rögzíteo kupak, Der Standard cikke alapján 2024. 08. 16.
[17] Új terepen veti be magát a MOHU www.vgh.hu 2024. 08. 10. 20.01.

offices and legislation were created to prevent this. During this period, the reaction of legislators was to ban isolated and isolated polluting activities and to regulate economic activities, because they believed that environmental pollution was a segmented and isolated phenomenon. However, the climate change at the end of the last century has completely transformed environmental legislation, which can only be tackled in a much more complex way. Politicians, civil activists and environmentalists around the world have realised that countries can only achieve their sustainability and climate protection goals through a series of coordinated and internationally harmonised legislative instruments. However, they also recognised that the means of national legislation and effective action by governments are determined by the combined material, cultural, political, legal and economic capacities of states, and that there may be internal limits to harmonisation, resulting in a diversity of environmental instruments. Based on these external and internal realities, the legal instruments for environmental protection that states can use can be divided into three main groups: the adoption of international treaties, the creation of binding domestic legislation and the creation of positive incentives to support the environmentally friendly actions of consumers, citizens and firms. It was in the 1970s that it was recognised that the voluntary commitment and informal or soft legal incentives described in the previous chapter were insufficient to tackle increasingly serious global problems. Following this realisation, national legislation and international standards and conventions began to be developed, still relying on a wide range of instruments from binding legal norms to recommendations and professional standards for their implementation.

The role of binding or prescriptive rules

As the idea of environmental protection has spread, a growing number of politicians have recognised the need for a system of binding legislation to reduce environmental damage, with a categorical ban on certain activities that are highly dangerous for the geographical or social environment. The problem is that there are few programmes around the world that enable people of average wealth or poverty to take action to protect the environment. Everyone knows it is a waste to flush toilets with clean drinking water, but the costs of using grey water and rainwater for this purpose are costs that no one wants to bear and governments do not want to subsidise. In addition to the few good examples, such as the application of the principle of sustainability in public procurement, the compulsory thermal insulation of new buildings, the compulsory provision of sewerage and the insulation programme for old houses, there are also many *bad and damaging measures* and accidental or deliberate fraud. An example of ill-considered and damaging legislation in Hungary is the Government Decree 221/2024 (31 July) on plug-in hybrid vehicles, which withdrew all the parking, running and tax benefits previously granted to this type of car, with the result that sales of low-carbon cars fell immediately. It should also be noted

that the Hungarian government has for decades subsidised the use and purchase of electric cars with money and tax incentives, while the professional judgement of this programme is controversial, as these cars are useful locally but are among the big polluters globally with their production and batteries. The Hungarian government is not alone in taking this measure, as Germany suspended its programme to promote the purchase of electric cars in December 2023, whereas previously it had subsidised the purchase of hybrid and fully electric cars to the tune of €10 billion over seven years, and had also provided tax incentives for them. Subsidies were used for 90% of the purchase of these types of vehicles. The measure has led to an 8-10% annual decrease in the sales of new cars in Germany.[18] It seems that in Europe, without public support, i.e. Community money, electric cars are not competitive in the market and without significant budgetary support, demand for them will fall.[19] According to Péter Szebenyi, in a certain sense it is already greenwashing to put a green label on an electric car without thinking about it, because the production process is very polluting. The mining of the battery raw materials needed to make them work creates a huge ecological footprint and there is no meaningful answer as to what will happen to the ageing batteries.

The phenomenon of greenwashing as a failure of legislation

As a consequence of incomplete or dysfunctional legislation, business actions or forms of action that only appear to help the environment have emerged, and their range of instruments and forms is incredibly diverse. Therefore, *greenwashing* is the practice whereby a for-profit company, in its communications or advertisements about its products or the environmental impact of its operations, states, suggests or implies specific or general statements that may be used to influence the decisions of customers, investors or other stakeholders, and fails to independently substantiate its claims and promises of environmental benefits in a way that is verified by research and publicly available, understandable and easily accessible to all[20]. The phenomenon of greenwashing has been triggered by the fact that the demand for environmentally friendly products in world markets has been rising steadily for decades and 85% of retailers have reported an increase in the concept of sustainable products, leading to an increasing number of companies offering green or so-called green products. According to the Nielsen polling company, even in the moderately committed and low-income Hungarian market, sixty-six per cent of consumers would pay more for environmentally friendly products than for non-sustainable ones, while many of these claims are exaggerations, distortions or half-truths. Many companies that abuse sustainability use jargon and scientific terms unknown to the average consumer in their marketing campaigns, or throw

[18] Piac és Profit 2024. október 5.
[19] Nem fogynak jól az elektromos autók, kétségbeesett üzenetet küldtek az európai autógyárak, Portfolió 2024. 09. 19.
[20] Tudatos Vásárlók Egyesületének definíciója alapján

around pseudo-jargon that does not exist. Consumers can be misled by the very fact that a product's packaging says that the cocoa beans come from a sustainable farm, because the average consumer may be confused by the fact that there are over 500 eco-labels of different quality and origin on the global market, while it takes the average consumer 7 seconds to decide which product to put in their shopping basket. This is why the European Commission is preparing to set stricter standards in a directive banning the use of unproven, vague and misleading environmental claims. A prime example of this misrepresentation is the 'vegan' comb, which did contain zero animal ingredients, as it was made of 100% plastic, but veganism cannot be an essential attribute for a hairbrush. The environmental benefit should be relevant and determinative so something irrelevant to the environmental impact should not be communicated by the manufacturer or retailer. At first glance, it is possible to distinguish between the certified and non-certified versions of a brand. Do not look exactly the same, and do not use exactly the same slogans and calls to action within the same brand for environmentally certified and non-certified products. Do not highlight product characteristics that are required by law for all products in the relevant product category in the EU market, because this does not give the product concerned an additional environmental benefit compared to other products. The advantage of the EU Ecolabel is that the assessment criteria apply to the whole life cycle of the product - including production and packaging waste management - and are laid down in legislation for each major product group. Products applying for the label are assessed by independent institutes. The suitability for use of these products is tested by the manufacturers themselves in independent laboratories or according to a pre-defined methodology and the documentation is submitted to the eco-label certification procedure.

A general approach to the effects of greenwashing

From an economic point of view, greenwashing can be described as a false marketing or public relations strategy in which a company is presented as taking responsibility for environmental protection, while no meaningful steps towards achieving these goals can be demonstrated in the actual operations of the company. As a result of their behaviour, dishonest firms gain an undue advantage in the marketplace, causing a loss of business to firms that have invested in truly green operations or in the development of environmentally friendly products, because the benefits in the price of green products are skimmed off by the firms making the false claims, giving them an undue competitive advantage. *In legal terms,* greenwashing is a message that misleads consumers, which can circumvent sustainability standards and thus constitute an unfair commercial practice against consumers. The essence of this act was formulated in the Hungarian Act XLVII of 2008 as follows: greenwashing is *morally* reprehensible because the corporate strategy is based on deceiving the bona fide consumer by persuading the well-intentioned consumer to make bad choices,

while they believe they are making the right choice and supporting sustainable and fair trade and the planet's wildlife, but in fact they are victims of unfair commercial practices. The first step towards market cleansing would be to stop companies from rating themselves and their products, because the environmental or sustainable nature of a good is a complex matter, involving many elements from composition to packaging to functional suitability. Such labels could only be used and only those products could be labelled as environmentally friendly or sustainable if they were certified as such by independent certification bodies that have assessed the essential characteristics of the product on a number of essential characteristics, for example by an EU eco-label such as the EU ecolabel.

The most common forms of greenwashing

Over the past decades, many forms of bad faith behaviour by companies have emerged, ranging from seemingly innocuous minor lies to major inaccuracies to deliberate and malicious deception of consumers, but there are also countless other forms of greenwashing strategies.

A common form of *greenwashing* is for companies to present elements of their normal business practice as a sustainability step. This was the case with the Fiji Islands hotel where the concept of greenwashing was first articulated by an American environmentalist in 1986. The activist noticed a sign in his hotel bathroom that he was using the same towel for several days to protect coral reefs. After a brief investigation, he concluded that the environmental protection was a smokescreen, because the hotel's real aim was to save money by washing less. For management, sustainability was only important if it gave them a financial advantage[21]. A no less deceptive form of greenwashing was reported by the head of the Hungarian Circular Point, who said that in larger companies, circular products are used in a way that does not cannibalize, i.e. displace, conventional products, "but rather has a marketing function, while most products operate according to a linear economic model".[22]

A particular form of greenwashing is *greencrowding,* or hiding in the crowd effect, where a company or national government joins a group with a loud name and hides in the crowd, moving at the speed of the slowest member to adopt green policies, slowing the group itself. As an example, the NGO Planet Tracker cited the Alliance to End Plastic Waste (AEPW), which has brought together the activities of sixty-five companies and included among its members the biggest oil giants, ExxonMobil and Shell, which are certainly pro-environment, as well as market leaders in plastic packaging and food multinationals such as Pepsi Cola. Astonishingly,

[21] Császár Barna: Greenwashing-a szállodai törölközőtől a zöld finanszírozásig, DLA Piper Hungary
[22] Kákos Anna: Sosem lesz körforgásos a gazdaság, amig a jogszabályok nem kényszerítik ki – hvg.hu 2022.06.15.3.

eight of the top twenty single-use plastics producers were members of AEPW[23]. This explains the low effectiveness and weak sanctions against the use of plastic products.

Greenlighting, a method in which participants emphasise their green ambitions in an overall communication strategy and focus on a particularly green feature of a company's operations or products in an attempt to divert attention from the company's environmentally damaging activities elsewhere. In the case of Toyota, for example, the production of zero-emission vehicles accounted for only 0.2 percent of total sales in 2021. This is the lowest proportion of the world's 10 largest car manufacturers, yet their communication campaign is full of slogans like "beyond net zero", "the future is electric" and the like. A similar strategy was followed by fast food chains switching to straws made from recycled paper, who continued to work with meat suppliers responsible for destroying forests.

Taxation as a tool for climate protection

Green taxes began to be used more widely in the second half of the 20th century, when it was recognised that taxes could not only provide revenue for the budgets of modern states, but could also influence the behaviour of economic agents and individuals. Following this recognition, sustainability aspects were added to traditional economic policy objectives in the tax systems of pro-environmental states[24]. From an environmental point of view, *green* or *environmental taxes* are public revenues, mainly from central government budgets, including levies, charges, duties and all other types of public tax, which have a direct impact on the protection of the environment, an indirect impact on its state or an impact on the way in which economic operators use environmental resources and transform their natural environment. In contrast to this definition, a much more practical approach, which quantitatively captures the regulatory objective, is reflected and applied in Regulation (EU) No 691/2011. According to the EU standard, which is almost entirely devoid of value judgements, an environmental tax is a type of public charge based on a physical unit of something that has a proven negative impact on the environment, regardless of the name given to it by the Member State. The reason for this legislative approach may be that environmental taxes vary considerably from one Member State to another in terms of their name, purpose, rate and method of levying, and therefore few common legislative elements or detailed objectives to be defended can be identified that would be acceptable to all countries[25]. The only common characteristic of the type of taxes that support land protection can be identified is that they aim to bring about change in the way human societies consume and

[23] Nagy Nikoleoa: A greenwashing olyan, mint a hidra, Telex, Techtud 2023. 03. 21. 1-3
[24] Bögöthy Zoltán-Hausmann Róbert: Új, zöld és fenntartható adórendszer 17. fejezet 526-527
[25] Bartha Ildikó-Bordás Péter-Horváth M. Tamás: Hős és antihős: környezel politika és pénzügyi szabályozás Pro futuro 2020/2. 130. 132

produce by using legal instruments to improve the state of their environment[26]. With environmental taxes, whatever form they take, Oates argues that countries achieve double gains because they can both reduce pollution levels in corporate production and increase revenues for the tax system[27]. According to a joint database of the OECD and the European Environment Agency, in 2003, countries on average collected 2-2.5% of their GDP in this form, which represented 6-7% of tax revenues[28]. However, this share has unfortunately declined in recent years and in OECD countries only 1.5% of GDP and 5.1% of tax revenues were derived from this source in 2021. Green tax revenues represent 0.7% of GDP in the US budget and 0.6% of GDP in China[29]. These figures are likely to reflect the level of commitment to environmental responsibility in a given country, as expressed by "the amount of resources devoted to environmental protection and their use in budget revenue and expenditure".[30] For some decades, the economic idea has been spreading that by using financial means to protect the land, legislators can restore the overall social supply and demand balance that has been disrupted by environmental pollution. This is the solution followed by the polluter pays principle, which was formulated in 1920 by an English economist called Pigou, based on the idea of compensation for negative effects, but is also enshrined in Article 191(2) of the Treaty on the Functioning of the European Union.[31] To apply this idea effectively in practice, we need to know who is directly responsible for pollution. In practice, we see that governments are often lenient on polluters in the interests of the budget, a phenomenon we can observe in Hungary, where environmental pollution from battery and mobile phone manufacturing plants is treated rather laxly by the government, partly because according to the KSH data, in 2006 the additional burden of polluting products, batteries and packaging materials generated a significant 4.9 billion[32] in revenue for the budget. In terms of the mechanism of economic impact, this means that governments, representing the interests of the community, make polluters pay the price for the harmful consequences of their activities and the negative social impacts, while they are not aware of the real cost of the damage and the penalties do not always reflect the extent of the damage. What is certain, however, is that production that damages nature will at some point become unsustainable at the price of green taxes, and that a high price will reduce the consumption and production of such products, thereby mitigating the negative impacts of harmful activities on the community. Based on this line of thinking, the bulk of green taxes today are levied on the economic operators responsible for pollut-

[26] Tanyi Anita: A környezetvédelmi adók gazdaságtan, Levegő Munkacsoport 2007. március, 1-2
[27] Oates: Green Taxes, Southern Economic Journal, 1995. Vol 61. No. 6. 507. /Alex 76.
[28] Tanyi Anita: i.m. 1
[29] OECD Report 2021. cited in Bögöthy Zoltán-Hausmann Róbert: i.m. 554
[30] Bartha Ildikó-Bordás Péter-Horváth M. Tamás: Hős és antihős: környezel politika és pénzügyi szabályozás, Pro futuro 2020/2. 130.
[31] Bögöthy Zoltán-Hausmann Róbert: i.m. 543.
[32] Népszava.hu 05. 09. 2019.

ing emissions[33]. However, the restriction of production can only be fine-tuned and flexible, because green taxes have the unintended effect of reducing production and employment and thus also fiscal revenues.

Types of environmental taxes

According to a joint database of the OECD and the European Environment Agency, in 2007 there were 375 environmental taxes and 250 environmental charges in countries around the world, and they have been a growing group of taxes ever since. Environmental taxes can be grouped into four main types according to the EU criteria: energy taxes, pollution taxes, resource taxes and transport taxes. However, the financial burden of these taxes is disproportionately distributed between the different types of taxes, with an EU average of 77.7% of tax and levy revenues from energy taxes, 19.05% from transport taxes and only 3.25% from pollution and resource taxes, according to a 2018 report.[34]

Energy taxes include public charges levied on the extraction of energy and on energy products ready for consumption on the market. They include excise duties, i.e. taxes on gas and petrol and other petroleum derivatives, but also taxes on coal, natural gas and electricity used in energy production, which are effectively single-phase consumption taxes, and carbon emissions and trading. The bulk of energy taxes are excise duties on fuel for internal combustion engines, and are therefore seen by many as the most effective climate protection instrument. These taxes will reach 26% of petrol and 21% of diesel prices in India in 2023, while in the US the tax will be 12% on petrol and 15% on diesel. In Turkey, the rate is 20% and in Hungary it exceeds 30% of the price of fuels.

The second element of the green tax is the *pollution tax, which is* levied on air and water pollution and use, as well as on companies that increase noise pollution and waste treatment companies. These environmental taxes work by making the extra costs of landfilling more expensive, thereby encouraging operators to reduce inputs and increase recycling. Research has shown that incineration is even more dangerous than landfilling if the technology is not right, so taxes are also being used to encourage recycling.

Resource taxes are levied on the use of natural resources that can be exhausted, such as water, forests, flora and fauna, but also on the use of land for the protection of land not connected to the sewerage system, on the withdrawal of land from agricultural production (land protection levy) and on the use of pesticides in agricultural production. A common form is the water use tax or rainfall tax, which is levied on households and businesses alike. These taxes have caused major social conflicts in developing countries, such as the tax on rainwater harvesting in Bolivia, but also include some types of taxes, fees and charges linked to land ownership, levied after

[33] Bögöthy Zoltán-Hausmann Róbert i.m. 545

[34] Bartha Ildikó-Bordás Péter-Horváth M. Tamás: Hős és antihős, Pro Futuro 2020/2. i.m. 133.

the transformation of the landscape and environment, the abandonment of agricultural land or deforestation. A new element could be the fertiliser tax or load tax introduced in Finland on pesticides until 2007 and 1994 respectively, which were intended to protect the soil and reduce environmental pressure. Sweden also applies such taxes, which are not levied on agricultural producers but on manufacturers and importers on the basis of the active substance content of the fertiliser. Since the tax was introduced in 1984, sales of artificial active substances in agriculture have fallen by 50%[35]. Norway introduced the pesticide tax as early as 1988, which has reduced their use by about 35% in thirty years.

A large group of green taxes are *transport taxes, which* are linked to the ownership and use of any means of transport and in many cases even include environmentally friendly electric cars. The registration tax on cars, invented and pioneered in France and introduced in Hungary within two years of its introduction, falls into this category. This group of taxes includes motor vehicle taxes based on engine power. In 2018, the Swedish government introduced a bonus-malus system, where vehicles are ranked on a scale according to their average carbon dioxide emissions, where the lower the vehicle's emissions value, the lower the vehicle tax. This group includes the much-debated air transport tax, from the air passenger tax to the airline seat tax introduced in Norway in the 1970s, to the increase in the special tax on airline tickets.

Problems in the practical application of green taxes

The question of the effectiveness of the green tax system

The first and most important question about green taxes is *their effectiveness,* i.e. their ability to make financial standards suitable for achieving the environmental objectives set. However, legislators must recognise that the market can adapt to different types of green taxes to different degrees. The effectiveness and efficiency of environmental taxes is primarily determined by the elasticity of consumer demand, i.e. the form and extent to which producers and consumers are able to respond to the imposition of the tax.[36] As a general principle, consumer demand for the basic products that human communities need to sustain their way of life - fuels, drinking water, air, heating fuels, food - is rather inelastic. Wang et al. found that for gasoline and diesel, customers will hardly restrain consumption if they become more expensive, but in the long run, in theory, consumption may fall[37]. An excellent Hungarian example of elastic demand was given by Kerekes, who found that demand for propellant dispensers fell immediately because of a tax on them.[38] Generally speaking,

[35] Szívós Alexander: A zöld adók kézirat 115.
[36] Bögöthy Zoltán-Hausmann Róbert: i.m 549
[37] Wang et al. 2016.
[38] Kerekes Sándor: Környezetgazdaságtan, A környezetszennyezés gazdaságtana 9.5 1998.

in most national markets elastic demand is only present for non-essential products such as crisps, spirits, cigarettes, luxury goods, paints, clothing. An excellent example of a successful and complex approach to environmental taxation is the effective taxation of plastic bags in shops in several countries, introduced in Ireland in 1999 as a 'bag tax' on plastic packaging. The impact of this type of tax has reduced the use of polluting and poorly biodegradable bags everywhere and experts believe that the taxes are achieving their aim.[39]

Legal problems in imposing green taxes

The application of green taxes can be hampered by effective lobbying and effective legal action by multinational companies, which in all cases are backed by the ancient tax principle that only the old tax is a good tax, and therefore any new tax imposed is considered illegal by the bearers of that new burden. Exxonmobil, one of the world's largest oil and gas companies, has launched a high-profile lawsuit against the European Union to block the entry into force of an extra-profit tax imposed by the EU on its annual profits, with a 33% deduction[40]. The tax would have been levied on companies that profited heavily from the energy crisis, to use the revenue to support small firms and households in difficulty. The US company challenged the EU's right to levy taxes in court, not the level of the tax, and thus questioned the legitimacy of any public tax, which also affects environmental taxes. These measures are not labelled environmental and were clearly introduced to increase budget revenues[41]. The problem is that consumers and businesses are unable to distinguish between the many other similarly named environmental taxes already paid by taxpayers and the new burden, thereby reducing their compliance with green taxes. He pointed out that, to take advantage of the tax dumping, in 2021, the Municipality of District XVIII introduced a 1,000 forint air passenger tax on passengers arriving at or departing from the airport, partly to reduce energy prices and partly to reduce noise and other pollution in the environment. The regulation has been challenged by the government office and Budapest Airport[42]. In the lawsuit, the municipality pointed out that many other European cities have implemented such a tax, in the Netherlands, Germany and Norway. One of the fundamental issues of green taxation is to assess its impact on sectoral competitiveness. "In France, the reform of the energy tax was rejected by the Constitutional Court in December 2002, saying that it was contrary to the principle of equal treatment enshrined in the French Constitution." the more energy-intensive a company was, the greater the reduction in its tax base, which for the most polluting companies meant a reduction of up to 95%."[43]

[39] Anita Tanyi: i.m. 5
[40] Csurgó Dénes: Beperli az EU-t az Exxonmobil az extraprofitadó miatt, 444.hu, 2022. 12. 29.
[41] Molnár Szabina-Rál Emese-Ilku Miklós: Közel 10 ezer forint különadót vetnek ki a repjegyekre index.hu 2022. 06. 05.
[42] Tamásné Szabó Zsuzsanna: Felügyeleti eljárást kezdeményezett az ezerforintos légiutasadó miatt a Budapest Airport. 24.hu 2023. 01. 31
[43] Anita Tanyi: i.m. 4-5.

Problems of social support for green taxes

An important issue for environmental taxes is their social acceptability, as voluntary compliance can help achieve the aim of the legislation, but gaining the support of communities poses a number of problems. The effectiveness of green taxes is determined by the views of leading politicians, experts and media actors who often appear in the media to shape the views of communities. A bad example is the US, where some leading Republican politicians do not support green principles, support oil extraction in Alaska and the Gulf of Mexico, allow fracked natural gas extraction and deny the process of climate change. Perhaps it is because of these views that people have not supported carbon taxes, and in Washington State in 2016 and 2018 they refused to raise carbon taxes, while in France in 2018 they forced the government to abandon the tax.[44] Among European countries, Switzerland and Austria have taken the approach of imposing a carbon tax and having distributors pass it on to consumers. In Switzerland, the carbon tax was phased out in 2008 and has been steadily increased, but the aim has been to compensate the public.[45] In Indonesia, 2-2.8% of GDP was allocated to gasoline subsidies until 2008. When this was abolished and average excise taxes were introduced, social subsidies were increased, public education was improved and the small and medium enterprise (SME) sector was supported. In Iran, the government subsidised fuel use until 2010, when it was abolished and fuel taxes were used to launch an environmental awareness campaign and spend on energy efficiency improvements. 20% of the increase in green tax revenue was used for public sector, education, hospitals and half of the additional revenue was distributed as a monthly subsidy to almost everyone. These government measures turned energy taxes into a social issue, thereby diverting public attention from environmental goals and ultimately using the extra revenue for non-environmental purposes. The basic principle with green taxes is that their adoption is greatly enhanced by an understanding of the environmental problem."[46] Apart from the Iranian government, few governments have followed this principle and little effort has been made to educate the public about environmental problems and explain the purpose of climate protection measures. Politicians should provide real information to the public, because political acceptance of certain measures depends on perceived fairness. It should also be seen that simply introducing new green taxes or raising the rates of old energy taxes will not help save the planet.

There may also be a problem of compliance if nations bear an unfair share of the burden of climate change. For example, India's burden is four times greater than its share of responsibility. However, since states do not bear the burden themselves, it is ultimately the population that pays for the unfair distribution of costs.

[44] Drews-Van Bergh: What explains public support for climate policies? Climate Policy, 16, 2016. 855-856.
[45] Levegő Munkacsoport: Valódi megoldás az üzemanyagár csökkentése helyett, levegomunkacsoport. blog.hu 2022. 09. 13.
[46] Tanyi Anita: A környezetvédelmi adók gazdaságtana, Budapest 2007. Levegő Munkacsoport anyaga 7.

Conclusion

In my work, I have reviewed the legislative and fiscal processes relating to environmental protection and analysed some of the instruments that are frequently used. I found that voluntary protection of our environment is a good but not sufficient means to achieve sustainability goals. Voluntarism can only be effective in two cases. On the one hand, at a macro level, in developing countries' environmental commitments, and on the other hand, at a micro level, in influencing individual consumption, voluntary compliance can be effective if communicated through simple messages that are understandable to all. In my work, I briefly described the next stage of climate protection, in which international organisations have defined the environmental tasks and principles for national legislatures. I then analysed the functioning and effectiveness of the different legal instruments, starting from soft and essentially dispositive regulatory elements and ending with categorical legal prohibitions. I presented the impact of greenwashing on economies and land protection and identified its different manifestations. I have found that explicitly prohibitive norms are the most effective weapons for environmental protection because, if they are based on thorough impact assessments and well-defined rules and expert work, they can significantly reduce the environmental pressures on societies. It can be argued that revising environmental rules alone, rethinking production and consumption in a sustainable and circular way, can be effective in protecting the environment. There is huge and untapped potential in the regulation of productive enterprises. In today's globalised world, international organisations should not only provide for a global minimum tax, but also for globally sustainable production targets and conditions. In the main part of my work, I have examined the functioning and actual environmental impacts of eco or green taxes and found the following. Despite the existence of several reliable definitions of green taxes, accepted by experts, countries apply them in different forms and to different degrees, with the result that national green taxes and tax systems are not comparable. We also have to face the fact that many tax laws that have an environmental or health protection objective are not at all suitable for fulfilling the defined climate protection task. The strongest bad example of this inefficiency is the environmental impact of excise duties, which are included in energy taxes, and which is highly questionable. Just because a standard has a good earth-saving purpose does not make it effective and efficient. "The imposition of green taxes is not always the right answer to the problem at hand, and other options should be carefully examined."[47] I also noted that in the application of green taxes, priority should be attention should be paid to consumption flexibility and differential treatment of essential consumer goods. It is also very important that other legal options should be explored before imposing the tax and that green taxes should only be applied if it seems the most appropriate solution, as in the case of the bag tax. An important finding of my research was that

[47] Anita Tanyi: i.m. 5.

in most cases, significant environmental results can be achieved if green taxes are introduced in combination with other environmental policies of a different nature.[48]

We need to see that global pollution problems can only be solved through international cooperation and harmonised, partly tax-based, rules. National governments could only decide on the actual size of the tax, within a 'tax to' limit, according to the economic and financial situation of the country concerned. The global minimum tax should be followed as an example to follow in regulation. Taxation can have a place among environmental instruments, but only if it is introduced in a conscious and complex way, after real and sustainable alternatives have been created.

The final and summarising conclusion of my work is that taxation is always a cultural phenomenon, and therefore green taxes can only be effective in a well-mannered, educated and environmentally conscious society. Poorly applied environmental taxes are only an unnecessary extra burden on taxpayers, increasing their budget revenues, reducing tax morale and failing to support the cause of environmental protection.

Due to the topicality of the subject, I found it necessary to consult a number of press articles as well as relevant academic publications.

I have arranged the references used in alphabetical order.

References

1. Bartha Ildikó – Bordás Péter – Horváth M. Tamás: *Hős és antihős: környezeti politika és pénzügyi szabályozás,* Pro Futuro, 2020
2. Bíró Ágota: *Greenwashing, azaz a zöldre mosás jelentése és típusai,* 2021. 11. 29. – Download
3. Bögöthy Zoltán – Hausmann Róbert: *Új, zöld és fenntartható adórendszer*, MNB kutatás, 17. fejezet
4. Brundtland Report, ENSZ, 1987
5. Crutzen – Stoemer – Steffen: *The Future of Nature*, Yale University Press, 2000
6. Császár Barna: *Greenwashing – a szállodai törölközőtől a zöld finanszírozásig,* DLA Piper Hungary, 2021. 10. 18. – Download
7. Csomor Zsolt: *Értelmetlen találmány a rögzített kupak,* Der Standard alapján, 2024. 08. 16. – Download
8. Csurgó Dénes: *Beperli az EU-t az Exxonmobil az extraprofitadó miatt,* 444.hu, 2022. 12. 29. – Download
9. Drews – Van Bergh: *What explains public support for climate policies?*, Climate Policy, 2024. 08. 17. – Download
10. Európai Tanács: *Sajtóközleménye,* 2024. 02. 05. – Download

[48] Tanyi Anita: i.m. 7.

11. Global Footprint Network, 2021 (idézi Bögöthy Zoltán – Hausmann Róbert)
12. Kákos Anna: *Sosem lesz körforgásos a gazdaság, amíg a jogszabályok nem kényszerítik ki,* hvg.hu, 2022. 06. 15. – Download
13. Kerekes Sándor: *Környezetgazdaságtan,* 1998
14. Kiss József: *Biztos jelek, amelyek a birodalmunk bukásához vezetnek,* G7.hu, Élet Világ, 2023. 12. 29. – Download
15. Lemostuk a szégyent – Románia tisztább, Maszol.ro, 2024. 09. 24. – Download
16. Levegő Munkacsoport: *Valódi megoldás az üzemanyagár csökkentése helyett,* levegomunkacsoport.blog.hu, 2022. 09. 13. – Download
17. Marnitz István: *Kifogytunk a nyersanyagokból,* Népszava, 2021. 12. 20. – Download
18. Molnár Szabina – Ráti Emese – Ilku Miklós: *Közel 10 ezer forint különadót vetnek ki a repjegyekre,* index.hu, 2022. 06. 05. – Download
19. Nagy Nikoletta: *A greenwashing olyan, mint a hidra,* Telex, Techtud, 2023. 03. 21. – Download
20. Oates: *Green Taxes*, Southern Economic Journal, 1995
21. Portfolió.hu: *Nem érdekli a román cégeket a környezetvédelem,* 2023. 02. 03. – Download
22. Portfolió.hu: *Nem fogynak jól az elektromos autók,* 2024. 09. 19. – Download
23. PWC: *Szakmai anyag,* 2018
24. PWC: *Ha a kör bezárul – a körforgásos gazdaság jelentősége és lehetőségei,* 2018
25. Sarkadi-Illyés Csaba: *Miniszter az e-autókról,* azonnali.hu, Economix, 2024. 08. 21. – Download
26. Szívós Alexander: *A zöld adók kézirat*
27. Tamásné Szabó Zsuzsanna: *Felügyeleti eljárást kezdeményezett az ezerforintos légiutasadó miatt a Budapest Airport,* 24.hu, 2023. 01. 31. – Download
28. Tanyi Anita: *A környezetvédelmi adók gazdaságtana,* Levegő Munkacsoport, 2007. március
29. Tudatos Vásárlók Egyesülete: *Definíció alapján*
30. vgh.hu: *Új terepen veti be magát a MOHU,* 2024. 08. 10. – Download
31. Zádori Bence: *Elérte Norvégia azt, ami máshol még csak álom,* Economx.hu, 2024. 09. 19. – Download
32. Zsuppán András: *A Szajnát igenis megtisztították,* Válasz online.hu, 2024. 08. 15. – Download

Éva Ladányi[1]

Shadow Warriors on the Silk Roads: Assassins, Fedayeen, and Beduin in Middle Eastern Irregular Warfare[2]

Abstract:

This study examines three iconic martial cultures of irregular warfare in the Middle East: the medieval Nizari Isma'ili Assassins, the 20th-century Palestinian Fedayeen movements, and modern Jordanian Beduin special units. The aim of this historical and cultural comparison is to reveal the tactics (e.g., patterns of self-sacrifice, loyalty, and decentralized warfare), motivations, and socio-cultural impacts of these non-state armed groups, comparing them within the context of contemporary proxy wars occurring along geopolitical fault lines. It analyzes how these forms of asymmetric warfare connect to historical military routes, such as the Silk Roads and other strategic paths, and to what extent they have influenced and continue to influence regional stability and broader security risks, including health hazards. Special attention is given to the issue of epidemic transmission along military routes, which is relevant both in the historical context of the Silk Roads and in modern conflict zones. Utilizing an interdisciplinary approach-combining historical, military, cultural, and epidemiological perspectives-this study contributes to a deeper understanding of irregular warfare in the Middle East. Finally, the paper highlights that a thorough understanding of the dynamics of irregular warfare is indispensable for managing future global conflicts and hybrid threats.

Keywords: Irregular warfare, asymmetric warfare, Middle East, Assassins, Fedayeen, Beduin warriors, Silk Roads, geopolitics, non-state actors, proxy wars, security risks

[1] The author is an Honorary Assistant Professor at the Medical School of the University of Pécs (PTE ÁOK) and serves as the Co-Chair of the Space Working Group at HM EI Ltd., a strategic entity of the Hungarian Ministry of Defense. Holding advanced degrees in Theology, Canon Law, and Nuclear Energy Law, she is a recognized expert in state building and the hawala banking system, with extensive publications in these fields. Her interdisciplinary research focuses on the intersections of religious, legal, and security paradigms, and the strategic and public health impacts of irregular conflicts. Her work integrates agricultural sciences and complex biological systems.

[2] This article is a secondary publication. The original version was published in Acta Lunae, Vol. 1, No. 1 (2026), ISSN 3141-706X. https://jardin-de-la-lune--a-hold-kertje.webnode.hu/acta-lunae/

Introduction

The global security environment of the first quarter of the 21st century is defined by armed conflicts such as the war in Ukraine and the ongoing clashes within the Israeli-Palestinian-Iranian complex. These conflicts are frequently interpreted as proxy wars, where regional and global actors appear as influential factors beyond the immediate combatants. The United States, the European Union, China, Russia, Iran, North Korea, and the states of the Persian Gulf and the Levant contribute to the dynamics of these theaters through arms shipments, intelligence sharing, diplomatic pressure, or the support of non-state actors and irregular groups. This complex environment, situated along geopolitical fault lines, underscores that alongside traditional interstate warfare, asymmetric and irregular warfare maintains its critical relevance.

From this perspective, it is particularly timely to re-examine the activities of non-state armed groups that have been present in Middle Eastern history for centuries. The medieval Assassins, the 20th-century Fedayeen, and Beduin warriors provide three prominent examples of irregular warfare that have left a profound mark on the region's formation, not only from a military standpoint but also socio-culturally and ideologically. The activities and *modus operandi* of these groups have significantly impacted both power structures and social dynamics.

This study examines these three historically distinct yet functionally parallel movements within a comparative analytical framework. Particular emphasis is placed on how they contributed to phenomena spreading through human mobility and interconnectivity, specifically at the intersections of historical military routes-such as the Silk Roads-and modern conflict zones. The objective of this research is not merely to uncover historical analogies but to understand how these types of martial cultures and associated mobility patterns shape regional geopolitical stability and broader security risks, including public health concerns-both in the past and the present-taking into account the dynamics of epidemic transmission along military routes. This article highlights the complexity of irregular warfare, the role of cultural myths, and why a thorough understanding of this phenomenon is essential for addressing the geopolitical challenges of the 21st century.

The Conceptual Framework and Historical Dimensions of Irregular Warfare

The concept of irregular warfare remains one of the most complex and contested categories within military science and international relations. Classical warfare models-premised on open confrontations between conventional state militaries-are increasingly inadequate for interpreting both modern and historical conflicts, particularly within the Middle East. Irregular warfare encompasses armed activities conducted by non-state actors, decentralized groups, or ideologically motivated militias, often employing asymmetric means while bypassing traditional conventions of war.

The roots of this phenomenon extend back to antiquity: the Jewish Zealots, Scythian raiders, and various tribes labeled "barbarians" by the Romans all utilized combat tactics that fell outside the military norms of their era. In the Middle Ages, the emergence of the Nizari Isma'ilis (commonly known as the Assassins) in the Islamic world represented a deliberate shift toward a strategy based on clandestine, targeted political eliminations. In the modern era, guerrilla warfare, partisan movements, urban insurgencies, and sectarian militias represent diverse manifestations of irregular conflict. This historical continuity underscores that asymmetric approaches are not merely products of the modern age, but rather timeless manifestations of the adaptive strategies employed by the militarily disadvantaged.[3]

Distinctions Between Regular and Irregular Forces

The distinction between regular and irregular forces is not solely organizational or tactical; it is fundamentally legal and moral in nature. The Geneva Conventions, for instance, are only partially applicable to irregular combatants, posing significant challenges to international law. Regular armies typically operate under state legitimacy, with a unified command structure and within international legal frameworks, particularly concerning the laws of war *(Ius in Bello)* and human rights norms. In contrast, irregular forces often lack official status, and their activities frequently fall into a "gray zone" between terrorism, insurgency, and international law[4]. However, irregular warfare is not inherently illegitimate[5]: colonial liberation movements, national resistances, or the self-defense organizations of religious communities often fall into this category, and history frequently validates their legitimate aspirations.

The Rise of Non-State Actors and Their Role in Geopolitics

The Middle East has been a particularly fertile ground for various forms of irregular warfare, partly due to the region's tribal structures, religious diversity, and the power vacuums resulting from colonial and post-colonial transitions. These factors have contributed to a complex environment where non-state actors have been able to gain significant military and political influence, frequently challenging dominant state actors.

In the post-Cold War era, non-state actors-including militias, guerrilla groups, and religious fundamentalist organizations-play an increasingly vital role in regional and global security policy. The following sections examine three martial cultures

[3] Metz, S., & Millen, R. (2004). Insurgency and Counterinsurgency in the 21st Century: Reconceptualizing Threat and Response. Strategic Studies Institute.

[4] Hoffman, F. (2007). Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies.

[5] Clausewitz, C. von (1832). Vom Kriege [A háborúról]. Magyarul: Zrínyi Kiadó, 2014.

Criterion	Assassins (Alamut)	Fedayeen (20th Century)	Jordanian Beduin Special Units
Period	11th–13th Century	From the 1950s	20th Century to present
Location	Persia (Iran), Alamut	Palestine, Jordan, Lebanon	Jordan
Leadership	Hassan-i Sabbah	Multiple organizations (e.g., Fatah)	Under the Hashemite Monarchy
Objective	Religious-political influence	Palestinian statehood, struggle against Israel	State stability, border defense, royal protection
Term for Warrior	*Fidā'ī* (self-sacrificer)	*Fedayeen* (self-sacrificers)	Beduin soldiers, elite units
Ideology	Isma'ili Shiite Islam, mystic-political	Arab nationalism, Palestinian self-determination	Tribal loyalty, monarchist patriotism
Notes	Secret society, hierarchical organization	Guerrilla warfare, international visibility	Elite formations, Western training, royalist loyalty

Figure 1: Comparative Table of the Three Organizations. Source: Author's own work

that operated across different historical eras yet shared a common logic, highlighting the diversity and adaptive capacity of irregular warfare: the medieval Assassins, the 20th-century Fedayeen, and the modern Jordanian Beduin special units.

The Assassins: Nizari Isma'ilis Fighting in the Name of Faith

The Fortress of Alamut and the Legacy of Hassan-i Sabbah

One of the most enigmatic and frequently cited irregular combat organizations of the medieval Middle East is the Nizari Isma'ili community, often referred to in Western historiography as the „Assassins" (Latin: *assassini*). The movement emerged at the end of the 11th century, centered at Alamut Castle in modern-day Iran, under the leadership of the charismatic and radical Hassan-i Sabbah († 1124), who represented a militant branch of Isma'ili Shiite Islam.

As illustrated in Figure 2, the topography of the Nizari state was a series of isolated points connected by secret lines, which stood in sharp contrast to the river-like, linear movement of the Silk Road. This structural arrangement allowed them to intervene effectively in global processes, while the intersections of their network, such as the surroundings of Masyaf and Alamut, became zones of heightened epidemiological risk due to military mobility.

Figure 2: Decentralized network of Nizari Ismaili (Assassin) fortresses and the topological comparison of the linear Silk Road trade route (11th–13th centuries). The sketch illustrates secret communication (faint dashed lines) and the conflict points (red spikes) where military movement and epidemic risk intersected. Source: Own editing

Religious Doctrine, Political Objectives, and the Tactics of Targeted Assassination

The Assassins' combat strategy fundamentally diverged from the prevailing military norms of the era. They did not maintain a conventional army, nor did they engage in open-field battles. Instead, they executed clandestine, targeted political assassinations-frequently in public spaces-to demonstratively instill fear and instability. These executions were typically carried out with daggers, and the operatives-known as *fidāʾī*s-rarely expected to survive their missions.

The term *fidāʾī* literally translates to „one who sacrifices himself" in Arabic, embodying a doctrine of religious martyrdom within the Assassin context. Warriors underwent prolonged ideological and spiritual conditioning. According to popular legends, Hassan-i Sabbah constructed a „paradise" behind the fortress, where recruits were allegedly drugged with hashish and led to believe that dying in service would grant them immediate entry into heaven. While the historical veracity of these accounts is debated, the role of psychological manipulation and religious fervor is undeniable.

The Archetype of the "Sacrificial Warrior" in Historical and Mythic Contexts

The Assassins operated for over a century and a half, significantly impacting the course of the Crusades. Both Crusader leaders and Muslim rulers became targets

of their operations. The Nizari political entity was eventually dismantled during the Mongol conquests; Alamut Castle was razed by the forces of Hulagu Khan in 1256.

The legacy of the Assassins, however, transcended their own historical epoch. The image of the „secret sect of killers" became deeply embedded in Western culture. This archetype continues to be reinterpreted in modern media-most notably in Vladimir Bartol's novel *Alamut* (1938) and the *Assassin's Creed* video game and film franchise.

The Fedayeen: The Dawn of Modern Guerrilla Movements in Palestine

The Birth of Palestinian Resistance Movements and the Role of the Fedayeen in National Identity

The term „fedayeen" (Arabic: فدائيون, singular: *fidāʾī*) literally translates to „those who sacrifice themselves." Since the mid-20th century, this concept has become the hallmark of Palestinian guerrilla movements, particularly following the 1948 Arab-Israeli War. This conflict resulted in the displacement of hundreds of thousands of Palestinians into refugee camps across Jordan, Lebanon, and other Arab states.

Initially, the fedayeen operated as decentralized, grassroots groups conducting raids against Israeli military and infrastructural assets. The movement rapidly evolved into a cornerstone of Palestinian national identity, gaining further momentum in the 1960s with the rise of Fatah and the Palestine Liberation Organization (PLO).

A 1969 *Time* magazine report described the fedayeen navigating the Jordan Valley under the cover of night, moving-as one operative put it- "like cockroaches," driven by the conviction that clandestine warfare was their only recourse. One commando stated: *"I do not like this stealthy war. But we have no choice. There is no army to fight beside us"*. Lacking a conventional military structure, these guerrillas frequently executed operations independently, often with minimal external support.

Feature	Assassins	Fedayeen
Place of Origin	Persia (modern-day Iran), Alamut Castle	Modern fedayeen primarily in Palestine, though the term's etymology is rooted in Persia
Period of Emergence	11th Century (c. 1090)	Modern Palestinian fedayeen from the 1950s; however, the term has been in use since the Middle Ages

Feature	Assassins	Fedayeen
Historical Link	Hassan-i Sabbah utilized the term *fidāʾī* to describe his devoted warriors	Modern fedayeen adopted the designation, though they are not direct descendants of the Assassins

Figure 3: Historical and Geographical Origins Source: Author's own work

Tactical Evolution: From Guerrilla Warfare to the International Political Arena

The tactics employed by the fedayeen integrated classical guerrilla warfare with modern information operations. Targets included Israeli military outposts, oil pipelines, and transport infrastructure; the movement also gained international notoriety through aircraft hijackings. According to the *Time* report, guerrillas from the Popular Front for the Liberation of Palestine (PFLP) successfully sabotaged the Aramco Trans-Arabian Pipeline, which connected Saudi Arabia to Lebanon via Israeli-controlled territory.

The activities of the fedayeen also posed significant internal challenges for neighboring Arab states. In Jordan, the Palestinian guerrillas began to establish a parallel power structure, a development that ultimately culminated in the events of Black September in 1970, when King Hussein's forces conducted a large-scale military crackdown on Palestinian armed factions.

Distinguishing Myth from Reality in the Portrayal of the Palestinian Fedayeen

Within the refugee camps, the figure of the fedayeen was elevated to a heroic archetype for the younger generation. Children frequently expressed the aspiration: *"I want to be a fedayeen when I grow up"*. Simultaneously, however, the movement was plagued by internal fragmentation and rivalries between factions, while tensions with host nations (such as Egypt, Jordan, and Lebanon) led to profound crises of legitimacy.

The *Time* report suggests that the Al-Fatah leadership had even prepared contingency „contracts" targeting Arab leaders-including President Nasser and King Hussein-should the host countries exert excessive pressure on their operations. This dynamic illustrates that the fedayeen were engaged in a multi-front struggle, contending not only with Israel but also navigating their own complex political environment in a bid for survival and dominance.

In a Middle Eastern political landscape where heightened rhetoric is common, the fedayeen appeared resolute in their mission: *"We will fight-if necessary, even against our Arab brothers. We will accept nothing less than the return to Palestine"*.

Beduin Warriors: Desert Traditions and Integration into Modern Armies

The Military Heritage of Beduin Tribes and Their Role in Middle Eastern History

The Beduin-semi-nomadic, Arabic-speaking tribal communities of the Middle East-have been pivotal actors in the region's military and political landscape for centuries. Their adaptation to the harsh desert environment, coupled with exceptional mobility, survival skills, and tribal cohesion, fostered a martial culture uniquely suited for irregular warfare.

While Beduin warriors participated in campaigns as far back as the early Islamic conquests, they gained particular international prominence during the Great Arab Revolt (1916–1918). During this period, they fought against the Ottoman Empire under the guidance of British officer T. E. Lawrence (popularly known as „Lawrence of Arabia"). The Beduin tactical repertoire-characterized by rapid raids, concealed movement, and an intimate mastery of the terrain-can be regarded as a precursor to modern guerrilla warfare.

The Case of Jordanian Beduin Special Units: From Tribal Loyalty to Professional Military Discipline

Jordan represents a unique case study in the modernization of Beduin military traditions. The backbone of the nation's armed forces is comprised of the Hashemite Royal Guard, the Desert Force, and other elite echelons, which are largely recruited from Beduin tribal backgrounds. These units serve a dual purpose: beyond their primary military functions, they are essential to political stability, as the legitimacy of the Hashemite monarchy rests significantly upon the enduring loyalty of the Beduin tribes.

The King's Guard, for instance, is far more than a ceremonial body; it is an elite combat force tasked with the direct protection of the Sovereign. While the training of Beduin personnel now aligns with rigorous international standards, they have successfully preserved their distinct cultural identity, manifested in their traditional attire, specific weaponry, and the continued respect for tribal hierarchies.

Adapting Beduin Martial Culture to Modern Warfare and State Structures

The trajectory of Beduin warriors illustrates how a traditional, tribe-based martial culture can be integrated into a modern, centralized state military. However, this process of adaptation has not been without friction; tensions occasionally arise between the demands of state centralization and the preservation of tribal autonomy and traditional loyalties.

Nonetheless, the Jordanian model stands as a successful example of synthesizing irregular combat traditions with professional military frameworks while maintaining cultural heritage. This remains particularly relevant in parts of the Middle East where state institutions are fragile, and social cohesion is often anchored in tribal or communal allegiances rather than national identity alone.

Modern Irregular Networks: Case Studies from Iraq, Syria, and Lebanon

The Diversity of Militias and Paramilitary Groups in Post-Conflict Regions

In the post-conflict regions of the Middle East, the erosion of state structures has facilitated the rise of various irregular armed groups. These militias often transcend purely military functions, assuming social and political roles and establishing parallel institutional frameworks that operate alongside or in place of state organs. The organizational structures of these militias are highly diverse: some are mobilized along ethnic or sectarian lines, others are sustained by external patronage, while some have evolved from local self-defense units into significant regional players.

Case Studies: Hezbollah, the Mahdi Army, and Syrian Militias – Religious, Ethnic, and Political Motivations

- Hezbollah (Lebanon): Supported by Iran, this Shiite organization has become a dominant force in Lebanese political and military life. It is characterized by a potent combination of religious ideology, comprehensive social services, and substantial military capabilities.
- Mahdi Army (Iraq): A Shiite militia led by Muqtada al-Sadr that gained prominence during the American occupation. It has since evolved into a political movement, though its armed wing remains an active influence.
- Syrian Militias: The civil war catalyzed the formation of numerous paramilitary groups, including the pro-government National Defence Forces (NDF), as well as various Kurdish, Sunni, and Alawite militias. These entities frequently operate with foreign backing (e.g., from Iran, Russia, Turkey, or the USA).

The Phenomenon of "Militia States" and the Regional Influence of Non-State Actors

The concept of the „militia state" describes political entities where non-state armed groups perform not only military but also governance functions. These structures often function in parallel to state institutions. Hezbollah, for example, manages its own healthcare, education, and social welfare networks in Lebanon. Similar pat-

terns are observable in Iraq and Syria, where militias often act as the primary providers of local security and justice.

The regional influence of non-state actors is particularly pronounced in the proxy wars between Iran and Saudi Arabia, where militias serve as geopolitical instruments. These dynamic poses novel challenges to international law, peacekeeping operations, and the traditional Westphalian concept of sovereignty.

Name	Founded	Ideology	Area of Operation	External Patrons	Political Role	Military Capacity
Hezbollah	1985	Shiite Islamism, pro-Iran, anti-Israeli	Lebanon (primarily South Lebanon and Beirut)	Iran, partially Syria	Parliamentary party, government positions, social services	Thousands of fighters, rocket systems, guerrilla warfare expertise
Mahdi Army	2003	Shiite nationalism, anti-Western, Iraqi sovereignty	Iraq (Baghdad, Najaf, southern regions)	Iran (formerly); currently mixed support	Political movement (Sadrist Movement), parliamentary presence	Thousands of fighters, experienced in urban combat
Syrian Militias	Since 2011	Mixed: Alawite, Shiite, Sunni, Kurdish – often pragmatic	Syria (nationwide; notably Aleppo, Homs, Damascus)	Iran, Russia, Turkey, USA (depending on the group)	Limited; primarily local administrative and security roles	Variable: light weaponry, local defense, reinforced by external support

Figure 4: Comparative Table – Irregular Militias in the Middle East. Source: Author's own work

Health and Epidemiological Risks Along Military Routes and Modern Conflict Zones

Historically, military and trade routes-such as the Silk Roads-served not only as conduits for cultural and economic exchange but also as critical channels for the spread of pandemics. Troop movements, merchants, and displaced populations significantly accelerated the transmission of infectious diseases like plague, cholera, and typhus, resulting in profound demographic and social upheavals.

In modern conflict zones, characterized by irregular networks and forced migration, similar public health risks emerge. Collapsed healthcare infrastructure, deteriorating hygienic conditions, water scarcity, and overcrowded refugee camps create ideal environments for the spread of pathogens. The mobility of militias and armed groups further facilitates the regional transmission of diseases, exacerbating humanitarian crises and generating additional security challenges. This nexus underscores

that military conflicts possess deep-seated social and health dimensions that must be integrated into security policy analysis and strategic responses.

The Myth of the Shadow Warrior in Culture and Media

The Figure of the "Holy Warrior" in Literature and Pop Culture

The archetype of the irregular warrior-whether an Assassin, a Fedayeen, or a modern militiaman-is frequently portrayed in culture as the „warrior for a sacred cause" (Holy Warrior), an individual acting against established power structures out of moral or religious conviction. This topos is particularly prominent in the following works:

- Vladimir Bartol: *Alamut* – This novel explores the history of Hassan-i Sabbah and the Assassins, offering a profound philosophical examination of faith, manipulation, and freedom. In the name of a „sacred mission," the protagonists commit political assassinations while the boundaries between reality and illusion are systematically eroded.
- *Assassin's Creed* (Ubisoft) – This video game franchise and its film adaptations recontextualize the mythology of the Assassins for a modern audience. Players take on the role of members of a secret society fighting against systemic oppression, blending historical facts with speculative fiction. The narrative frequently reflects on the philosophical dilemmas of liberty versus order and chaos.

The Tension Between Romanticization, Propaganda, and Reality in Modern Depictions

Cultural representations often idealize irregular warriors, attributing to them heroism, self-sacrifice, and moral superiority. However, this romanticization frequently obscures the complexities of the ground reality:

- Romanticization: The shadow warrior as a „freedom fighter" acting on behalf of the people is a recurring motif in both Western and Eastern narratives.
- Propaganda: Modern militias-such as Hezbollah or the Mahdi Army-utilize their own media outlets to construct an archetype of the martyr-hero, serving both recruitment and domestic legitimacy.
- Reality: In the field, these groups are often implicated in violence against civilians, sectarian cleansing, or political repression. Cultural representations rarely reflect this inherent ambivalence.

Work Title	Genre	Year of Release	Type of Warrior Depicted	Ideological Background	Level of Realism
Alamut	Novel	1938	Assassin	Islamic fundamentalism, mysticism	Medium
Assassin's Creed	Video Game / Film	2007–	Secret society warriors	Liberty vs. Control, Anarchism	Low
Paradise Now	Film	2005	Suicide bomber	Palestinian nationalism	High
The Battle of Algiers	Film	1966	Urban guerrilla	Algerian War of Independence	Very High
The Old Guard	Film / Comic	2020	Immortal mercenary	Morality, justice, postmodern ethics	Low

Figure 5: Summary Table of Cultural Representations. Source: Author's own work

Concluding Remarks: Irregular Warfare in Global and European Contexts

Geopolitical Consequences and the Impact on International Security

In the 21st century, irregular warfare is no longer merely a military phenomenon but a complex dynamic embedded in social, political, and religious structures. It fundamentally challenges classical state-centric security paradigms. Non-state actors-militias, guerrilla groups, and shadow states-exert increasing influence over regional stability. This is particularly evident in the Middle East, where entities like Hezbollah, the Mahdi Army, or various Syrian militias have established parallel power structures, often evolving into legitimate political stakeholders.

These developments not only reshape the regional geopolitical balance but also challenge the institutional frameworks of international law and multilateral security cooperation. The proliferation of proxy wars, transnational armed networks, and unconventional warfare is redefining the concepts of sovereignty, intervention, and responsibility.

Hybrid Warfare and the Changing Face of Future Conflicts

Conflicts in the 21st century are increasingly hybrid in nature: traditional military force, cyberattacks, disinformation campaigns, economic coercion, and the activities of non-state actors have become inextricably intertwined. Irregular warriors-whether religious ideologues, nationalist militiamen, or mercenaries-often operate in the „Gray Zone," where the distinction between war and peace becomes blurred.

While cultural representations-such as *Alamut* or *Assassin's Creed*-frequently romanticize these figures, the reality is that such groups are often instruments of geopolitical manipulation, social fragmentation, and crises of legitimacy. On modern

battlefields-such as in Ukraine-non-state actors and irregular tactics are not merely supplementary; they are formative elements of the conflict.

Europe's Response: Strategic Awakening and Adaptation

For the European Union, irregular warfare is not only an external threat but a challenge to internal cohesion. Disinformation, political interference, migratory pressure, and cyber threats are tools utilized by both state and non-state actors to undermine the European security architecture. The EU's response-encapsulated in the Strategic Compass, the Hybrid Toolbox, and efforts to stabilize the Eastern and Southern Neighborhoods-indicates that the continent is undergoing a strategic awakening.

Europe has recognized that security policy is inseparable from social resilience, media literacy, and community cohesion. Countering hybrid threats requires a multidimensional approach involving diplomatic, economic, and cultural instruments alongside military ones.

Managing Complex Threats and the Need for an Interdisciplinary Approach

A key takeaway of this study is that irregular warfare is not solely a military issue. Analyzing historical examples and modern conflicts demonstrates that cultural, social, and health dimensions are as critical as the application of armed force. The spread of epidemics along military routes, social radicalization, and the role of cultural myths all suggest that future security policies must be interdisciplinary and preventative.

The past serves as a geopolitical mirror for the future: the examples of the Assassins, Fedayeen, and Beduin warriors show that decentralized, ideologically motivated, and socially embedded combat structures can shape power relations over the long term. Recognizing these patterns and integrating them into strategic thinking is essential for understanding the conflicts of the present and the future.

<u>Irregular Warfare</u>
- Historical Examples
  - Assassins
  - Fedayeen
- Cultural Representations
  - Alamut
  - Assassin's Creed
- Geopolitical Impacts
- Preventative Strategies
- Modern Militias

- Hezbollah
- Mahdi Army

– Hybrid Warfare

Summary of Findings: A Global Reinterpretation of Irregular Warfare and its European Implications

The security environment of the first quarter of the 21st century is increasingly characterized by the blurring of boundaries between conventional and irregular forms of warfare. The three historical martial cultures examined in this study-the Assassins, the Fedayeen, and the Jordanian Beduin special units-are not merely historical curiosities; they represent structural patterns that recur within contemporary hybrid warfare doctrines.

Through their decentralized organizational logic, ideological motivations, and deep social integration, these groups serve as archetypes for the non-state actors that play a decisive role in current conflicts. Militias organized along religious, ethnic, or political identities, as well as combat structures embedded in transnational networks, are redefining the concept of warfare and challenging the Westphalian state-centric security paradigm.

The irregular warfare patterns of the Middle East are particularly relevant in light of current global conflict dynamics. The war in Ukraine, as well as the proxy wars within the Israeli-Palestinian-Iranian complex, clearly demonstrate that the employment of non-state actors, disinformation operations, cyber warfare, and the weaponization of social polarization are no longer supplementary, but structural elements of modern warfare.

For the European Union, this development is not only a foreign policy challenge but a test of internal cohesion. Hybrid threats-including electoral interference, energy coercion, migratory pressure, and social disinformation-generate complex security challenges for which traditional military responses alone are insufficient. The EU's response-encapsulated in the Strategic Compass, the Hybrid Toolbox, and efforts to stabilize the Eastern and Southern Neighborhoods-can be interpreted as a strategic awakening aimed at strengthening resilience and enhancing collective response capabilities.

The interdisciplinary approach of this study-combining historical, military, cultural, and epidemiological perspectives-highlights that irregular warfare is a complex phenomenon that generates significant social and public health risks. Human mobility along military routes, the spread of epidemics, and the role of cultural myths all contribute to ensuring that irregular warfare remains a critical area of research and strategic inquiry in the 21st century.

One of the most vital tasks for future security policy will be the integration of historical experience, cultural sensitivity, and technological adaptation into a complex

response system. Such a system must not only react to but proactively shape the global security environment, including the guarantee of epidemiological preparedness and public health security.

Bibliography

Primary and Historical Sources

1. Bartol, Vladimir. 1938. *Alamut*. Ljubljana: Modrijan.
2. Daftary, Farhad. 1990. *The Isma'ilis: Their History and Doctrines*. Cambridge: Cambridge University Press.
3. Daftary, Farhad. 1994. *The Assassin Legends: Myths of the Isma'ilis*. London: I.B. Tauris.
4. Glubb, John Bagot. 1957. *A Soldier with the Arabs*. London: Hodder & Stoughton.
5. Hodgson, Marshall G. S. 1955. *The Order of Assassins: The Struggle of the Early Nizârî Ismâ'îlîs Against the Islamic World*. The Hague: Mouton.
6. Lawrence, T. E. 1926. *Seven Pillars of Wisdom*. London: Jonathan Cape.
7. Lewis, Bernard. 1967. *The Assassins: A Radical Sect in Islam*. London: Weidenfeld & Nicolson.
8. Time Magazine. 1969. "Guerrillas in the Jordan Valley." *Time,* June 20.

Palestinian Fedayeen and Modern Guerrilla Movements

1. Khalidi, Rashid. 2006. *The Iron Cage: The Story of the Palestinian Struggle for Statehood*. Boston: Beacon Press.
2. MiltonEdwards, Beverley, and Peter Hinchcliffe. 2001. *Jordan: A Hashemite Legacy*. London: Routledge.
3. Sayigh, Yezid. 1997. *Armed Struggle and the Search for State: The Palestinian National Movement, 1949–1993*. Oxford: Clarendon Press.

Modern Militias and Irregular Warfare

1. Haddad, Fanar. 2011. *Sectarianism in Iraq: Antagonistic Visions of Unity*. London: Hurst.
2. Lister, Charles. 2015. *The Syrian Jihad: AlQaeda, the Islamic State and the Evolution of an Insurgency*. London: Hurst.
3. Mansour, Renad, and Faleh A. Jabar. 2017. *The Popular Mobilization Forces and Iraq's Future*. Beirut: Carnegie Middle East Center.
4. Norton, Augustus Richard. 2007. *Hezbollah: A Short History*. Princeton: Princeton University Press.

Irregular Warfare Theory

1. Galula, David. 1964. *Counterinsurgency Warfare: Theory and Practice*. New York: Praeger.

2. Keegan, John. 1993. *A History of Warfare*. New York: Vintage.
3. Kilcullen, David. 2009. *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*. Oxford: Oxford University Press.
4. Mao, Zedong. 2000. *On Guerrilla Warfare*. Champaign: University of Illinois Press.

Epidemiology, Mobility, and Conflict

1. Barry, John M. 2004. *The Great Influenza: The Story of the Deadliest Pandemic in History*. New York: Penguin.
2. Farmer, Paul. 2003. *Pathologies of Power: Health, Human Rights, and the New War on the Poor*. Berkeley: University of California Press.
3. McNeill, William H. 1976. *Plagues and Peoples*. New York: Anchor Books.
4. World Health Organization. Various years. *Health in Conflict Settings*. Geneva: WHO.
5. Snowden, Frank M. 2019. *Epidemics and Society: From the Black Death to the Present.* New Haven: Yale University Press.

Silk Roads and Mobility Networks

1. Beckwith, Christopher I. 2009. *Empires of the Silk Road*. Princeton: Princeton University Press.
2. Frankopan, Peter. 2015. *The Silk Roads: A New History of the World*. London: Bloomsbury.

Engy Ibrahim[1]:

From Confrontation to Controlled Cooperation: The Coptic Orthodox Church and the Egyptian Regime During the Sadat and Mubarak Eras

Abstract:

This study examines the evolution of Church–state relations in Egypt during the presidencies of Anwar Sadat (1970–1981) and Hosni Mubarak (1981–2011), focusing on the Coptic Orthodox Church's responses to shifting political and religious dynamics. Under Sadat, relations were marked by confrontation as the state aligned with Islamist movements and marginalized Copts politically, economically, and socially.[2] During Mubarak's rule, Church–state relations shifted toward controlled cooperation, in which the Coptic Orthodox Church, led by Pope Shenouda III, negotiated limited concessions while the state maintained ultimate authority.[3] This study seeks to answer the central research question: How did Church–state relations transition from confrontation under Sadat to controlled cooperation under Mubarak, and what were the implications for the Coptic community? The objectives are threefold: to analyze state policies affecting Copts, to examine the strategies of Pope Shenouda III and the Church in navigating these policies, and to assess the broader social and political impact on Coptic identity and minority rights. The working hypothesis is that the transition from confrontation to controlled cooperation provided Copts with a more tolerable socio-political environment while preserving structural inequalities inherent in authoritarian governance.[4] Understanding this trajectory illuminates the interplay between religion, minority rights, and state power in modern Egypt.

Keywords:

[1] PhD student, School of History, Faculty of Humanities and Social Sciences, Pázmány Péter Catholic University.

[2] Ibrahim, S. E. (1993). The Copts and political participation in Egypt. In M. W. Daly (Ed.), The Copts in modern Egypt (pp. 73–94). Boulder, CO: Lynne Rienner Publishers.

[3] Beattie, K. J. (2000). Egypt during the Sadat years. New York, NY: Palgrave Macmillan; Tadros, M. (2009). *Vicissitudes in the entente between the Coptic Orthodox Church and the state in Egypt (1952–2007). International Journal of Middle East Studies, 41*(2), 269–287. https://doi.org/10.1017/S0020743809090612.

[4] Gabriel, J. (2013). The Copts and the revolution: Religious and economic impact in Egypt. Journal of Middle Eastern Studies, 45(2), 233–257; Hasan, M. (2003). Coptic activism and the Egyptian state: A historical overview. Journal of Middle Eastern Politics, 15(2), 45–67.

Historical Background

Post-Monarchy Egypt and Early Coptic Marginalization

After Egypt transitioned from monarchy to republic in 1952, the Coptic community experienced structural marginalization. Under President Gamal Abdel Nasser (1954–1970), Copts faced political exclusion, limited economic opportunities, and institutional discrimination. Political participation was restricted following the abolition of political parties, while socialist reforms and nationalization disproportionately affected Coptic-owned businesses and land.[5] Educational policies further privileged Islam, notably through compulsory religious instruction and restrictions at Al-Azhar University, reinforcing Copts' marginalization.[6]

Emergence of Religious Nationalism

Although Nasser promoted a secular Arab nationalist ideology, Islam became increasingly tied to national identity through legal, educational, and institutional reforms. Copts were systematically excluded from the military, key ministries, and political leadership roles, fostering the perception of Copts as religious "others". These structural inequities created the conditions for the politicization of religion in Egypt and set the stage for later Church–state dynamics.[7]

Transition to Sadat and Early Church–State Confrontation

When Anwar Sadat assumed the presidency in 1970, he introduced policies that emphasized Islamic identity in governance and society, partly to consolidate political legitimacy and counter leftist and Nasserist factions. Sadat's realignment heightened sectarian tensions, as Islamist groups gained influence while the Coptic Church, led by the newly elected Pope Shenouda III in 1971, faced increased pressure to defend its community. Pope Shenouda's activism during Sadat's presidency marked a shift toward political engagement, transforming the Church into a key factor in negotiating the rights and protections of Copts under an increasingly Islamist-aligned state.[8]

---

[5] Ibrahim, S. E., Gabra, G., & Atiya, A. S. (1996). The Copts of Egypt. London: Minority Rights Group International; Gabriel, J. (2013). The Copts and the revolution: Religious and economic impact in Egypt. Journal of Middle Eastern Studies, 45(2), 233–257.

[6] Makhlouf, N. (2020). Education and religious minorities in Egypt: Structural exclusion in public policy. Arab Education Journal, 12(3), 211–230.

[7] Wright, R. (1984). The politics of Egypt: State–society relations under Nasser and Sadat. Berkeley, CA: University of California Press.

[8] Beattie, T. (2005). *The Egyptian Coptic Christians: The Conflict between Identity and Equality*. Islam and Christian-Muslim Relations, 16(2), 155–166; Mitchell, R. P. (1993). *The Society of the Muslim Brothers*. Oxford University Press.

The Sadat era (1970–1981): period of confrontation

Political and Religious Context

Sadat's turn toward political Islam: When Anwar Sadat assumed the presidency after Nasser's death in 1970, Egypt embarked on a significant ideological transformation. Seeking legitimacy and a political base, Sadat aligned himself with Egypt's religious establishment and conservative social forces, including the Muslim Brotherhood. He used religion as a unifying and legitimizing force to counter entrenched leftist and Nasserist elements.[9] Sadat reversed Nasser's repression of the Muslim Brotherhood, releasing leaders and allowing their reintegration into public life. In return, the Brotherhood supported Sadat's early policies, particularly his alignment with Western foreign policy and suppression of leftist groups.[10] This rehabilitation facilitated a wider Islamist revival, including the expansion of Islamic societies on campuses and increased circulation of Islamic literature.

Figure 1: The Presidency of the Arab Republic of Egypt. (1977, November 20). Anwar Sadat praying at the al-Aqsa Mosque, Jerusalem [Photograph]. Bibliotheca Alexandrina, Memory of Modern Egypt Digital Archive. Downloaded: 18. August 2025

"Believer president" rhetoric and constitutional Islamization: Sadat referred to himself as the "Believer President" (al-Ra'īs al-Mu'min) in public discourse. His actions -praying in mosques, quoting the Qur'an, invoking divine support- reinforced this image, signaling Islam's centrality in governance. A pivotal development was the 1980 amendment of Article 2 of the Egyptian Constitution. The amendment elevated Sharia from "a source" to "the principal source of legislation".[11] This formalized Islam's

[9] Kepel, G. (1993). Muslim extremism in Egypt: The prophet and pharaoh. Berkeley, CA: University of California Press.

[10] Wickham, C. R. (2002). *Mobilizing Islam: Religion, activism, and political change in Egypt*. Columbia University Press. Beattie, T. (2005). *The Egyptian Coptic Christians: The Conflict between Identity and Equality*. Islam and Christian-Muslim Relations, 16(2), 155–166; Mitchell, R. P. (1993). *The Society of the Muslim Brothers*. Oxford University Press. Kepel, 1993

[11] Hasan, S. S. (2003). *Christians versus Muslims in modern Egypt: The century-long struggle for Coptic equality*. Oxford University Press, P. 144-145.

primacy in law, with implications for family, education, media, and civil matters, alarming both Copts and secular Muslims. Pope Shenouda III warned that the amendment risked legalizing inequality and undermining a multi-faith society.[12]

State Policies and Discrimination

During Anwar Sadat's presidency, Egypt witnessed a discernible pattern of discriminatory policies and marginalization directed at the Coptic Christian population.

Marginalization of Copts in Public and Security Institutions: Copts were increasingly marginalized within Egypt's state bureaucracy, particularly in the security apparatus, judiciary, foreign service, and senior administrative positions. Historically well-represented in elite professional circles, including the judiciary and civil service, Copts' presence sharply declined under Sadat. Copts accounted for less than 2% of key decision-making positions despite comprising approximately 10% of the population. This underrepresentation was especially pronounced in the Ministry of Interior and intelligence agencies, where informal security clearance processes barred Copts from advancement.[13] During the 1970s, public discourse increasingly associated national loyalty with Islamic identity. Christians were often portrayed as politically unreliable or less committed to Egypt's Arab-Islamic national identity, which Sadat actively promoted. Church leaders reported systematic rejection of Christian applicants from police and military academies and frequent denial of promotions in public institutions without formal justification. Although these policies were not codified in law, informal vetting mechanisms and state security practices effectively excluded Christians from sensitive positions.

Restrictions on Church Construction and Religious Expression: One of the most visible forms of institutional discrimination under Sadat was the severe restriction on church construction and renovation. These constraints stemmed from the 1856 Ottoman Hamayouni Decree and its amendments, particularly the 1934 Al-Ezabi regulations, which required ten conditions to be met before granting a church construction permit. Criteria such as proximity to mosques, objections from Muslim neighbors, and population statistics were often applied arbitrarily to block projects. Although Sadat publicly claimed to support religious freedom, his regime maintained these restrictions. Christians required presidential approval for even minor repairs on churches, whereas mosque construction was expedited and subsidized by the state. Mosque-building flourished during Sadat's presidency as a symbol of his alliance with Islamist forces, while Christian places of worship operated under

[12] Karas, S. F. (1985). *The Copts since the Arab invasion: Strangers in their land*. American, Canadian, and Australian Coptic Associations, P. 97.

[13] Tadros, M. R. I., El-Fiki, M. A., & Soliman, S. S. (1996). *The Copts of Egypt*. Minority Rights Group International, p.10.

constant threat of closure due to bureaucratic hurdles.[14] Coptic communities were further frustrated by recurrent failures of state security forces to protect churches from mob violence or sectarian attacks. Often, authorities attributed responsibility equally to both parties, even when Christians were clearly targeted,[15] documented widespread impunity for perpetrators of sectarian violence against churches, noting that few were prosecuted.

Rise of Islamist Groups and State Negligence

Growth of Violent Islamist Groups: The period witnessed the emergence of groups such as al-Gamaʿa al-Islāmiyya and al-Jihad, which initially developed as campus-based student movements but expanded into broader societal actors. These groups drew support from impoverished rural areas and disaffected urban youth. Sadat's tolerance and strategic encouragement of their growth were intended to weaken leftist and Nasserist influence in universities and civil society.[16] Al-Gamaʿa al-Islāmiyya's ideology emphasized jihad against secular and Westernized elites and targeted non-Muslims, especially Copts. Islamist groups propagated their vision of an Islamic state through sermons, pamphlets, and street-level mobilization. University mosques became centers of radicalization, where Islamist leaders trained and organized followers.[17] Sadat's promotion of himself as the "Believer President" implicitly endorsed Islamist rhetoric. Government policies allowing semi-autonomous operation of religious societies in universities facilitated resource mobilization and the expansion of Islamist influence.

Attacks on Copts and Christian Property: The state's permissive stance contributed to escalating attacks on Copts and their property. Notable incidents included:

- 1972, Khanka: Islamist students led a mob that burned a church and dozens of Christian homes.[18]
- 1975, Samalout (Minya Governorate): Destruction of a church and Christian properties following a local altercation.
- 1976, Alexandria: Christian shops burned after sermons by radical imams.
- 1977, Sohag Governorate: Violent attacks on Christians over a land dispute, framed by authorities as a "tribal conflict".

Christian-owned stores, bookshops, and schools were frequently targeted, while clergy faced harassment and families sometimes fled their communities. Prosecutions were rare, and the state often relied on informal "reconciliation sessions" instead of legal remedies, fostering a culture of impunity. During the 1977 "Bread

[14] Pennington, R. (1982). *The Copts in modern Egypt*. Middle Eastern Studies, 18(2), 161–180.
[15] Human Rights Watch. (1994). *Egypt: Religious discrimination against Coptic Christians*. Human Rights Watch.
[16] Kepel, 1993
[17] Wickham, C. R. (2002).
[18] Hasan, S. S. (2003). *Christians versus Muslims in modern Egypt.*

Riots", churches were vandalized amidst general unrest, reflecting how Islamist narratives had merged with broader socio-economic grievances.[19]

Inadequate Police Response and Judicial Impunity: State protection of Copts was minimal. Police often arrived after attacks, investigations were opaque, and officers occasionally witnessed assaults without intervention.[20] When cases reached the courts, acquittals or lenient sentences were common. Witness intimidation, withheld evidence, and sympathetic judges created an environment where extremist actions went unpunished.[21] Pope Shenouda III criticized the lack of protection and accountability, but government officials accused him of inciting sectarianism. Local governors and judicial authorities often shared Islamist sympathies, further marginalizing Christian residents. By the late 1970s, the state's accommodation of Islamist groups had backfired: these organizations gained extensive influence, contributed to sectarian polarization, and undermined national unity. This environment ultimately facilitated the assassination of Sadat in 1981 by members of al-Jihad, highlighting the dangers that Pope Shenouda III and the Coptic Church had repeatedly warned about.

Church–State Breakdown and Confrontation (Sadat Era, 1970–1981)

Pope Shenouda's and his criticism of Sadat's policies

Initial Cautious Optimism (1971): Sadat's early presidency sought to heal divisions left by Nasser.[22] Pope Shenouda III, enthroned November 1971, emerged as a defender of Coptic rights.[23] Early relationship deteriorated due to Sadat's turn toward political Islam and Islamist alliances.

Image: 2 Pope Shenouda III with Sadat: Unknown photographer. (ca. late 1970s). President Anwar Sadat with Pope Shenouda III during an official meeting in Egypt [Photograph]. Downloaded: 8. August 2025

[19] Beattie, K. (2000). *Egyptian Copts and the politics of change*. Lynne Rienner Publishers.
[20] Ibrahim, S. E., Tadros, M. R. I., El-Fiki, M. A., & Soliman, S. S. (1996). *The Copts of Egypt*. Minority Rights Group International.
[21] Human Rights Watch, 1994.
[22] Beattie, K. (2000).
[23] Karas, 1985.

Early Tensions (1971–1976): Shenouda emphasized "full citizenship" and opposed restrictions on church building.[24] Khanka, 1972: Islamist youths burned a Christian community center; government delayed response; Shenouda led delegation and publicly protested. 1973–1975: Shenouda criticized selective law enforcement and underrepresentation of Copts in security forces; Sadat limited his access to state media.[25] Samalout, Minya, 1975: dispute over Christian school escalated into mob violence; police delayed response, victims pressured to drop complaints.[26] By 1976, Sadat's alignment with Islamists, university mosque mobilization, and restrictions on Christian student groups escalated tensions.

Escalation (1977–1979): Sadat–Islamist alliance deepened; sectarian violence increased; Shenouda intensified defense of Copts. Bread Riots, January 1977: Churches vandalized, Christian businesses attacked; state minimized sectarian aspect.[27] 1978: Alexandria Christian conference highlighted discrimination, church construction restrictions, and Islamist incitement; Sadat privately warned Shenouda against "mixing religion with politics". 1979: Camp David Accords triggered Islamist anger; attacks on Copts increased, police response delayed.[28] Shenouda emphasized justice over symbolic national unity.[29]

Constitutional Crisis and 1981 Exile of Pope Shenouda III: 1980 constitutional amendments, Article 2 changed from "a principal source" to "the principal source" of legislation, formalizing Islamic state identity.[30] Shenouda warned these amendments undermined legal equality for Copts.[31] Church opposed amendments via pastoral letters and private appeals; Sadat dismissed objections, labeling Shenouda as a source of sectarian tension.[32] Post-amendment, church construction permits stalled (Minya, Assiut, Sohag), while mosque construction continued unimpeded.[33] By late 1980, the stage was set for confrontation; Sadat saw Shenouda as a political threat; Shenouda viewed constitutional Islamization and state inaction as existential threats to Copts.

<u>1981: Sadat's decision to exile Pope Shenouda and appoint a council of bishops</u>

In 1981, Church–state relations in Egypt reached a crisis point as rising anti-Coptic violence and growing Islamist agitation, coupled with state inaction, intensified tensions. Pope Shenouda III's outspoken criticism of discriminatory policies and state

[24] Keraza Magazine, Issue 36, 9 September 1972, p. 4-7.
[25] Ibrahim, Tadros, El-Fiki, & Soliman, 1996, P. 12.
[26] Keraza Magazine, Issue 15, 11 April 1980
[27] Beattie, K. (2000).
[28] Karas, 1985, pp. 230-231.
[29] Keraza Magazine, Issue 13, 30 March 1979.
[30] Beattie, 2000, p. 142
[31] Hasan, 2003, p. 205
[32] Wickham, 2002, p. 112
[33] Human Rights Watch, 1994, pp. 12–13

neglect of sectarian attacks positioned him in direct conflict with President Sadat, who accused the Pope of politicizing the Church and threatening national unity. Events such as Shenouda's restriction of Easter celebrations in 1978, combined with the 1980 constitutional amendments, heightened Sadat's distrust and reflected his broader strategy of Islamization and authoritarian consolidation.[34]

On September 5, 1981, amid the September Arrests targeting political dissidents, Sadat exiled Pope Shenouda III to the Monastery of Saint Bishoy in Wadi al-Natrun, revoked his official recognition, and appointed a council of bishops to manage Church affairs. Officially justified as a response to political interference, the move was widely seen as an attempt to weaken Church leadership and intimidate the Coptic community.

Widespread Coptic protests and sense of persecution: The exile intensified fears of religious persecution while Shenouda maintained spiritual influence from afar and drew international condemnation as a violation of religious freedom. His release in 1985 following Sadat's assassination underscored the exile's enduring significance in illustrating the interplay of religious identity, political authority, and minority rights under Sadat.

The Mubarak era (1981–2011): toward controlled cooperation

Mubarak's Reversal and Early Reconciliation

Image: 3 Mubarak: Encyclopaedia Britannica, Inc. (2009). Hosni MuEncyclopaedia Britannica, Inc. (2009). Hosni Mubarak [Photograph]. Encyclopaedia Britannica. barak [Photograph]. Encyclopaedia Britannica. https://www.britannica.com/biography/Hosni- Mubarak Downloaded: 16. August 2025

Hosni Mubarak's presidency, spanning three decades from 1981 to 2011, was a defining period for Egypt's religious and sectarian landscape. Following the fraught relationship between the Egyptian state and the Coptic Orthodox Church under Anwar Sadat, Mubarak adopted a policy often described as "controlled cooperation." This approach combined symbolic reconciliation and limited concessions with continued state oversight, balancing the regime's authoritarian priorities with the need to manage sectarian tensions.

[34] Kepel, 1993

Restoration of Pope Shenouda III in 1985: Mubarak's first significant move was the restoration of Pope Shenouda III in January 1985, widely interpreted as a gesture of goodwill toward Egypt's Coptic minority. This restoration symbolized a break from Sadat's confrontational stance and opened a new phase in Church–state relations. Saad Eddin Ibrahim (1993) notes that Mubarak's decision was pragmatic: "By reinstating Shenouda, Mubarak aimed to co-opt the Church's leadership, thereby stabilizing internal sectarian tensions and securing the loyalty of the Christian minority".

The restoration was not purely symbolic. Mubarak's government granted the Church limited freedoms, including permissions for church construction and more public religious celebrations.[35] However, these concessions remained tightly controlled, with the state retaining authority over Church affairs, including the appointment of bishops and clergy.

Symbolic Gestures of goodwill toward the Church: Following Shenouda's return, Mubarak's regime engaged in high-profile symbolic acts to project religious tolerance and national unity, such as attending Coptic events and issuing public statements emphasizing the Copts' role in Egyptian society. These gestures reinforced the Coptic community's sense of belonging and deflected domestic and international criticism. However, scholars argue that these acts also reinforced state control, with Mubarak positioning himself as the ultimate arbiter of religious affairs. observes: "Mubarak's public association with the Coptic Church was a carefully choreographed political performance that emphasized coexistence yet masked ongoing structural inequalities". This managed visibility exemplified the controlled cooperation model, social stability without genuine institutional empowerment.

Political calculus; co-opting the Church to stabilize internal tensions: Mubarak's approach was shaped by the need to manage Islamist opposition and sporadic sectarian violence targeting Copts. The regime viewed the Coptic Church as a strategic partner in maintaining social order. Ibrahim (1987) explains: "The state incorporated the Coptic Church into its political framework to prevent alienation and reduce the potential for sectarian conflict to destabilize the regime". This incorporation came with conditions: the Church was expected to remain politically quiescent and cooperate with government authorities. In return, it received limited protection and symbolic recognition. Pope Shenouda adopted a pragmatic stance, prioritizing national unity and social stability over political confrontation.

[35] Gabra, G. (1996). *Coptic Egypt: History and a guide*. The American University in Cairo Press.

Gradual Emergence of Controlled Cooperation

The state informally recognized Pope Shenouda as the de facto representative of the Coptic community. The Church increasingly acted as an intermediary in local sectarian disputes and as a provider of social services. Mubarak's regime selectively responded to Coptic demands, easing rules for repairs (but not new construction) of churches, while retaining control over appointments, security, and sensitive policy levers.[36] This arrangement preserved macro-stability but entrenched extra-legal mediation and maintained uneven legal equality.

Informal recognition of Shenouda as representative of the Coptic community
Rehabilitation and Centralized Access (1985–Early 1990s): - After Sadat's assassination, Pope Shenouda returned from exile in 1985, marking a reset in Church–state relations. Under Mubarak, the papacy became the principal channel through which the state engaged with Coptic concerns, sidelining other civic or political representatives. By the early 1990s, Shenouda had effectively become the state's main interlocutor on Coptic matters, enabling controlled communication while limiting broader community participation.[37]

State-Controlled Representation: - Political visibility for Copts was primarily mediated through state appointments rather than elections. Roles in the Shura Council and occasional ministerial positions were largely symbolic, ensuring that influence remained centralized in the presidency and the papacy rather than through independent or democratic channels.

Diaspora Coordination and External Signaling: - Shenouda's coordination with the Coptic diaspora in North America, Europe, and Australia allowed the state to manage international scrutiny more effectively. His longstanding ban on pilgrimages to Jerusalem after the 1979 Camp David Treaty further aligned the papacy with national priorities, consolidating his role as a trusted representative of the Coptic community.[38]

The Church as Intermediary in Sectarian Conflict and Provider of Social Services
Intermediary Role in Local Conflicts: - Throughout the 1990s, local authorities frequently used the Church to mediate after church burning, land disputes, or intercommunal tensions. Instead of legal prosecution, bishops and clergy brokered customary settlements, ensuring temporary peace but sometimes perpetuating impunity.[39]

---

[36] Tadros, M. (2009). *Vicissitudes in the entente between the Coptic Orthodox Church and the state in Egypt (1952–2007). International Journal of Middle East Studies, 41*(2), 269–287. https://doi.org/10.1017/S0020743809090612.

[37] Menza, M. F. (2021). *Citizenship and religious freedoms in post-revolutionary Egypt*. Religions, 12(7). https://doi.org/10.3390/rel12070516

[38] U.S. Department of State. (2001). *International Religious Freedom Report 2006: Egypt*. Bureau of Democracy, Human Rights, and Labor.

[39] Human Rights Watch, 1994.

Expansion of Social Services: - Under Pope Shenouda, the Church expanded its social infrastructure, providing clinics, schools, scholarships, vocational training, and seasonal relief programs. These initiatives not only addressed genuine community needs but also strengthened the Church's role as a gatekeeper of social and economic resources.[40]

State Encouragement of Church Welfare: - The regime supported the Church's social role as it helped contain grievances, particularly against Islamists who ran parallel services. This dual role – as mediator and welfare provider – was central to the controlled-cooperation model.

Mubarak's regime selectively responding to Coptic demands

Church Construction and Repair: - Despite the symbolic rhetoric of equality, practical reforms were limited. 1998: Authority to permit church repairs delegated from the presidency to provincial governors, improving procedural speed but maintaining discretion. 1999: Presidential Decree 453 placed repairs of mosques and churches under the 1976 civil construction code, theoretically equalizing treatment[41]: Further delegation confirmed governor-level oversight, but security services retained gatekeeping powers. While repairs became easier, construction of new churches remained tightly restricted due to longstanding laws.[42]

Security and Justice: - Churches were occasionally provided with security details, yet criminal accountability for attacks was inconsistent. Local reconciliations often replaced prosecution, maintaining state control while limiting legal protections.

Political Participation and Symbolic Gestures: - The regime periodically appointed Copts to the Shura Council or ministerial posts and publicly attended Coptic celebrations. These gestures enhanced visibility but did not address structural inequalities.

Limits and Challenges of Cooperation

The Mubarak-era framework of controlled cooperation operated through a managed triangle: the presidency set broad policies and granted high-level concessions without structural reform, security services and governors-controlled permits, associations, and local reconciliations, and papacy converted access into tangible benefits for the Copts while discouraging unrest. While this arrangement-maintained stability, it limited broad reforms and perpetuated discretionary governance. Internally, the Church's dominance in welfare and mediation strengthened clerical authority but constrained independent Coptic NGOs, political parties, and rights groups, oc-

[40] Kılıç, E. (2023). Social welfare and religious minorities: The case of the Copts in Egypt. Middle East Review, 55(1), 67–89.

[41] U.S. Department of State. (2005). *Country reports on human rights practices – Egypt.* Bureau of Democracy, Human Rights, and Labor.

[42] MEMRI. (2006). Egypt's new church repair law examined. Middle East Media Research Institute, Special Dispatch No. 1284.

casionally creating tension with state-sanctioned channels.[43] Pope Shenouda's alignment with national policies, including his Jerusalem pilgrimage ban, reinforced his role as a cooperative interlocutor, enabling selective concessions from the regime. By the late Mubarak period, although the Church was institutionally robust, core issues such as new church construction, legal equality, and the de-securitization of religious affairs remained unresolved. Reforms were limited, producing only partial improvements in church repairs and administrative.[44] The Arab Spring briefly disrupted this authoritarian management, yet widespread sectarian violence did not materialize, reflecting latent social cohesion. This framework of controlled cooperation remains key to understanding contemporary Church–state relations, minority representation, and sectarian dynamics in Egypt.[45]

Continued Exclusion from High-Level Government and Military Roles: Although a few Copts held visible ministerial positions – such as Boutros Boutros-Ghali as Foreign Minister under Sadat and later Youssef Boutros-Ghali and Maged George under Mubarak – Copts remained largely absent from the highest levels of the military, intelligence, and provincial administration. For example, the 2011 Maldives Freedom Report noted that under Mubarak, only one Coptic governor (Qena) out of 25 held such a post, while security apparatuses – including the police, army, and intelligence – remained almost exclusively Muslim. This structural limitation demonstrates that controlled inclusion did not translate into real decision-making power.

<u>Sporadic outbreaks of violence</u>

– *The Kosheh Massacres (1999–2000):* - One of the most severe breaches of state protection occurred in al-Kosheh, Upper Egypt. Communal clashes in January 2000 resulted in the deaths of 20–21 Copts, marking one of the worst sectarian attacks of the era.[46] Investigations revealed prior coercion by police, including the rounding up of roughly 1,200 Copts in 1998, use of torture, and forced confessions. Subsequent trials often ended in acquittals or lenient sentences, prompting outrage among the Coptic community. Bishop Wissa warned, "If the perpetrators…walk free, it will be seen as a green light to kill Christians".[47]

[43] Halbouni, F. (2019). *Between promise and disappointment: Coptic youth movements and the sectarian question after the Egyptian revolution* (Doctoral dissertation, Johns Hopkins University.

[44] World Wide Religious News. (2005, December 13). Church building regulations eased. World Wide Religious News. https://wwrn.org/articles/19813/

[45] Meital, C. (2016, October 6). Egyptian regime approves church construction law, satisfying Coptic Church; interfaith conflict continues (Inquiry & Analysis Series No. 1273). Middle East Media Research Institute (MEMRI). https://www.memri.org/reports/egyptian-regime-approves-church-construction-law-satisfying-coptic-church-interfaith

[46] Canadian Coptic Human Rights Forum (CLHRF). (1999, December 12). *Press release on attacks against Copts in al-Kosheh*.

[47] Christian Solidarity Worldwide (CSW). (2003, March 4). *Report on religious freedom violations against Egypt's Coptic minority*. https://www.csw.org.uk

– *Alexandria Church Bombing (2011):* - Although this occurred after the Mubarak era, the 2011 Alexandria church bombing, in which 23 worshippers were killed, illustrates the persistent vulnerability of Coptic communities. Reports suggest that security services were unprepared to prevent the attack, highlighting the ongoing limitations of Church–state coordination in ensuring protection.[48]

The Church's quietest stance in exchange for limited concessions: The Coptic Church frequently pursued quiet negotiation over public confrontation. In the case of al-Kosheh, Pope Shenouda supported Bishop Marcos in seeking justice but prioritized reconciliation rather than legal or political escalation. This strategic silence secured limited concessions, such as permission for repairs or targeted protection, but reinforced dependence on informal, discreet channels rather than public advocacy or institutional reforms.

Surveillance and Containment

Control over Media and Church Appointments: State oversight extended to Christian media. Press and broadcast outlets critical of religious policy or sectarian violence were subject to vetting and censorship, particularly in the early 2000s. Self-censorship became common, as leaders understood that criticism could result in sanctions or closure. While the papacy retained spiritual authority, the state influenced appointments of bishops and administrative officials. These selections were aligned with Cairo's preferences, ensuring compliance and curbing dissenting church leaders. This subtle but effective control shaped internal Church dynamics and limited the emergence of independent leadership.

During the Mubarak era, the Coptic Orthodox Church faced growing internal and external pressures that shaped its political engagement. These pressures included the rise of autonomous diaspora activism, the centralization of authority in the papacy, and a fragile modus vivendi between the state and the Church.[49]

Rise of Coptic Activism Outside the Church's Authority (E.g. Diaspora Lobbying)

From the late 1970s onward – intensifying after President Anwar Sadat's 1981 sidelining of Pope Shenouda III – Coptic activism increasingly developed autonomous organizational centers outside the Pope's direct authority, particularly in North America, Europe, and Australia. Diaspora advocates framed Coptic rights as an international human-rights issue, leveraging journalists, think tanks, and U.S. congressional hearings to pressure the Egyptian state.

[48] Fahim, K. (2011, February 14). *Egypt's Christians after the revolution*. *The New Yorker*. https://www.newyorker.com

[49] Iskander, E. (2011). *Sectarian conflict in Egypt: Coptic–Muslim relations and the challenge of democratization*. *Middle East Policy, 18*(2), 140–156. https://doi.org/10.1111/j.1475-4967.2011.00489.x

Key Dynamics

Trigger Events and Distance from State Coercion: The 1981 confrontation convinced many lay Copts abroad that domestic channels were blocked. Operating from liberal democracies, diaspora organizers could lobby freely without fear of state retaliation.

Organizational Learning and Issue Framing: By the late 1980s and 1990s, diaspora networks professionalized, compiling incident lists, producing English-language briefs, and linking sectarian attacks to rule-of-law deficits in ways aligned with Western advocacy frameworks.[50]

High-Visibility Lobbying Moments: U.S.-based activists petitioned Congress and the State Department regarding Shenouda's status and broader discrimination. Some supported legislation linking aid to religious freedom, while others, often aligned with Church guidance, cautioned against "internationalizing" the issue in ways that could provoke backlash in Egypt.[51]

This "outside-in" pressure raised Coptic visibility internationally but created tactical and narrative fissures. Pope Shenouda preferred quiet bargaining with the presidency, while diaspora activists emphasized public conditionality. This tension shaped nearly every major Coptic rights confrontation through the 2000s.[52]

When Sadat sidelined Shenouda in 1981, Coptic communities abroad - especially in the U.S., Canada, Europe, and Australia - recognized that domestic avenues for advocacy were limited. These diaspora communities became key actors in pushing for Coptic rights internationally.

Diaspora Organizations: Autonomous and non-ecclesiastical

During Sadat's presidency and the early years of Hosni Mubarak (1981–2011), several non-ecclesiastical Coptic organizations emerged:

- **Coptic Solidarity Group (CSG):** Focused on lobbying U.S. Congress to link American aid to Egypt with improvements in religious freedom.
- **Egyptian Coptic Association (ECA):** Documented attacks on churches and produced English-language reports for international human rights bodies.
- **Coptic Federation:** Served as a coordination platform connecting Coptic activists across North America, Australia, and Europe.

[50] The Tahrir Institute for Middle East Policy (TIMEP). (2021, March 15). *Church construction in Egypt: Progress and persistent challenges.* TIMEP. https://timep.org/reports-briefings/church-construction-in-egypt-progress-and-persistent-challenges.

[51] Jadaliyya. (2012, March 22). *Copts in Egypt: Between silence and activism.* Jadaliyya. https://www.jadaliyya.com/Details/26422/Copts-in-Egypt-Between-Silence-and-Activism.

[52] Knafo, S. (2020). *Coptic Christians and the Egyptian state: Diaspora activism and domestic politics.* Middle East Policy, 27(2), 102–117. https://doi.org/10.1111/mepo.12567.

These groups operated independently of the Church hierarchy, which sometimes preferred discreet negotiation with Cairo. Diaspora organizations instead used public advocacy – petitions, press releases, and congressional testimonies – o increase international pressure on the Egyptian state.

Lobbying and International Advocacy

Diaspora organizations leveraged Western liberal democratic frameworks to frame Coptic rights as a human rights issue:

- Engaging journalists and think tanks to report on discrimination.
- Lobbying U.S. Congress for conditional aid legislation tied to religious freedoms.
- Testifying at hearings on Egypt's human rights record.

In the 1980s and 1990s, diaspora activists successfully highlighted incidents such as church attacks and restrictions on religious education. Some groups criticized the Egyptian government publicly, while others coordinated with Pope Shenouda's office to avoid backlash. This created a strategic tension between "quiet diplomacy" favored by the Church and "public international pressure" favored by the diaspora.

Diaspora's Role under Mubarak

Hosni Mubarak's long presidency allowed for an expansion of diaspora activism:

- Access to global human rights forums, using reports and testimonies to pressure Egypt.
- Monitoring legislation and religious policies, advocating for reforms in church property rights, education, and security for Christian communities.
- Non-ecclesiastical organizations acting as watchdogs, independent of the Pope, collecting data on sectarian incidents and sharing them internationally.

However, Mubarak's government maintained close control over religious institutions inside Egypt, and diaspora activism was often portrayed as foreign interference, which sometimes limited the impact of their lobbying.[53]

Strategic Tensions and Ideological Divides

While diaspora groups emphasized public accountability and Western human rights norms, Pope Shenouda often preferred quiet negotiation to prevent state retaliation against Copts in Egypt. This created:

[53] Yefet, B. (2017). *National unity and Muslim attitudes toward the Coptic minority. Middle East Journal, 71*(3), 345–363. https://doi.org/10.3751/71.3.14

– **Organizational Fragmentation:** Multiple diaspora organizations sometimes competed for influence and legitimacy.
– **Narrative Divergence:** Differing strategies sometimes confused U.S. policymakers about the Church's stance.
– **Advocacy Dilemmas:** Public campaigns risked provoking harsher domestic policies by Cairo, while quiet diplomacy risked limited international visibility.[54]

Achievements and Limitations

Achievements

– Raised global awareness of sectarian discrimination in Egypt.
– Influenced U.S. foreign aid debates, with some conditional aid discussions tied to religious freedom.
– Created transnational networks that continue to influence Egyptian politics today.

Limitations

– The Egyptian government's sophisticated lobbying and media campaigns often undermined diaspora narratives.
– Fragmentation among diaspora groups reduced the coherence of advocacy.
– Reliance on U.S. and European political channels sometimes led to perceived over-internationalization of domestic issues.[55]

Summary

By the late Mubarak period, an implicit bargain had emerged between the Church and the state. The Coptic Church, led by Pope Shenouda III, avoided direct confrontation, discouraged mass mobilization, and publicly affirmed national unity, while the regime consulted the Pope, allowed controlled expansion of churches and charities, and signaled protection - but retained oversight through security agencies. This arrangement remained fragile due to several factors. First, security-state gatekeeping meant that the Interior Ministry could veto permits, associations, and media access, allowing implementation to stall even with presidential approval; extrajudicial reconciliations often replaced accountability in sectarian cases. Second, the politicized religious framework, particularly Article 2 of the 1980 constitution, normalized perceptions that equality claims threatened national identity, restricting

[54] Wasef, Y. M. (2022). *Coptic diaspora activism and its impact on Egypt's religious policies. Journal of Middle Eastern Studies, 54*(2), 112–130. https://doi.org/10.1080/00263206.2022.2045678.
[55] Zeitoun, C. (2012). *Apparition of Our Blessed Virgin Mary in Zeitoun, Cairo. The Catholic Pilgrim*. https://thecatholicpilgrim.wordpress.com/2012/06/26/apparition-of-our-blessed-virgin-mary-in-zeitoun-cairo/.

reform opportunities. Third, a fragmented activism ecology - where diaspora campaigns favored public conditionality and domestic church diplomacy preferred quiet bargaining - enabled the state to provide selective concessions without systemic reform. The net effect was a contingent accommodation characterized by visible papal authority, episodic presidential intervention, and periodic diaspora activism, yet persistent structural inequality in representation, policing, and access to public goods. Scholars emphasize that without rule-of-law reforms, neither quietist bargaining nor international advocacy could secure durable equality.

Comparative analysis: from confrontation to controlled cooperation

Aspect	Sadat Era (1970–1981)	Mubarak Era (1981–2011)
State Strategy	Confrontational: Instrumental Islamization, rollback of Nasserist policies, framing of Sadat as "Believer President," constitutional amendments emphasizing shari'a, securitized sectarian governance.	Controlled cooperation: Reinstated papacy as interlocutor, formalized consultative channels, selective concessions, security oversight maintained, sectarian incidents framed as local disturbances.
Church–State Conflict	Open confrontation: Shenouda criticized anti-Coptic violence, faced exile in 1981, bishops' council appointed, monitored clergy, politicized permits, grievances securitized.	Negotiated accommodation: Shenouda returned in 1985, mediated local conflicts, oversaw social services, received symbolic recognition, constrained by security vetoes, reconciliation substituted for legal accountability.
Church Strategy	Moral witness: Publicly condemned discrimination and violence, leveraged diaspora networks, high cost in exile and administrative control.	Pragmatic accommodation: Quietist bargaining, incremental gains in social services and church repairs, centralized authority increased bargaining power but limited lay activism, aligned with state narratives.
Mechanisms of Cooperation	N/A – primarily confrontation; state-imposed controls and sanctions.	Permit/property regime: Repairs allowed, new construction restricted. Reconciliation over law: Sectarian incidents mediated extra-legally. Selective appointments, symbolic inclusion. Ecclesiastical intermediation for welfare and conflict. Narrative management emphasized national unity.

Aspect	Sadat Era (1970–1981)	Mubarak Era (1981–2011)
Implications for Coptic Agency	Constrained by exile and securitized environment, limited access to state institutions, political activism suppressed.	Centralized papal mediation: predictable communication but limited civic pluralism, persistent underrepresentation in military, judiciary, and government; Church substituted for state services; diaspora advocacy sometimes conflicted with domestic strategy.
Long-Term Outcome	High confrontation, structural inequality reinforced, Church positioned as politically suspect.	Pragmatic but fragile modus vivendi: limited gains, visible authority, episodic presidential interventions, ongoing structural inequality in representation and legal protections.

Conclusion

Sadat's era reflected direct confrontation, with politicization of religion, the Pope's exile, and high sectarian violence. Mubarak shifted toward controlled cooperation, restoring Shenouda and positioning the Church as a state interlocutor. Despite symbolic recognition and limited gains, structural inequalities endured: Copts remained excluded from senior positions, faced restrictions on church construction, and were vulnerable to impunity in sectarian attacks.

The duality of empowerment and constraint illustrates the fragility of minority rights under an authoritarian regime: strategic accommodation offered the Church leverage and stability, but the state-maintained oversight and control. The transition from confrontation to controlled cooperation demonstrates both the adaptability of the Church and the persistence of systemic discrimination in Egypt.

References

1. Ansari, L. (1986). Egypt: The Islamic view of society and politics. London: I.B. Tauris.
2. Atlantic Council. (2011). Egypt's religious media under state control. Washington, DC: Atlantic Council.
3. Beattie, K. J. (2000). Egypt during the Sadat years. New York, NY: Palgrave Macmillan.
4. Beattie, T. (2005). *The Egyptian Coptic Christians: The Conflict between Identity and Equality.* Islam and Christian-Muslim Relations

5. Christian Today. (2003). Egyptian court acquits suspects in Kosheh massacre. Retrieved from https://www.christiantoday.com.
6. CSW. (2003). Kosheh Massacre update. Christian Solidarity Worldwide.
7. Eibner, J. (1993). Church, state, and sectarianism in contemporary Egypt. Middle East Journal, 47(1), 21–40.
8. Fahim, K. (2011, February 14). *Egypt's Christians after the revolution*. *The New Yorker*. https://www.newyorker.com.
9. Gabra, G. (1996). The restoration of Pope Shenouda III and Church–state relations in Egypt. Cairo: Dar al-Maaref.
10. Gabriel, J. (2013). The Copts and the revolution: Religious and economic impact in Egypt. Journal of Middle Eastern Studies, 45(2), 233–257.
11. Halbouni, A. (2019). Managing minorities: State strategies and religious communities in the Middle East. Middle East Policy, 26(4), 45–62.
12. Hasan, M. (2003). *Coptic activism and the Egyptian state: A historical overview*. Journal of Middle Eastern Politics, 15(2), 45–67.
13. Hasan, S. S. (2003). Christians versus Muslims in modern Egypt: The century-long struggle for Coptic equality. Oxford: Oxford University Press.
14. Human Rights Watch. (1994). Egypt: Violations of freedom of religious belief and expression of the Christian minority. Retrieved from https://www.refworld.org/docid/3ae6a7ec0.html
15. Ibrahim, S. E. (1987). Egypt: The tyranny of the polity. Boulder, CO: Westview Press.
16. Ibrahim, S. E. (1993). The Copts and political participation in Egypt. In M. W. Daly (Ed.), The Copts in modern Egypt (pp. 73–94). Boulder, CO: Lynne Rienner Publishers.
17. Ibrahim, S. E., Gabra, G., & Atiya, A. S. (1996). The Copts of Egypt. London: Minority Rights Group International.
18. Iskander, E. (2011). Sectarian conflict in Egypt: The media's role. Washington, DC: Atlantic Council.
19. Jadaliyya. (2012). Activism in the Coptic diaspora: U.S. advocacy and Church guidance. Retrieved from https://www.jadaliyya.com
20. Karas, S. F. (1985). The Copts since the Arab invasion: Strangers in their land. American, Canadian, and Australian Coptic Associations.
21. Kepel, G. (1993). Muslim extremism in Egypt: The prophet and pharaoh. Berkeley, CA: University of California Press.
22. Khalil, A. (1999). Coptic activism in exile. Journal of Religion and Society, 4, 1–23.
23. Kılıç, E. (2023). Social welfare and religious minorities: The case of the Copts in Egypt. Middle East Review, 55(1), 67–89.
24. Knafo, S. (2020). Diaspora lobbying and religious freedom in Egypt. Foreign Policy Analysis, 16(3), 345–366.

25. Knafo, S. (2020). Presidential discourse and the U.S. Coptic diaspora: Navigating religious and political identities. *Journal of Middle Eastern Studies, 42*(3), 123–145.
26. Makhlouf, N. (2020). Education and religious minorities in Egypt: Structural exclusion in public policy. Arab Education Journal, 12(3), 211–230.
27. Meinardus, O. F. A. (2002). Two thousand years of Coptic Christianity. Cairo: The American University in Cairo Press.
28. MEMRI. (2006). Egypt's new church repair law examined. Middle East Media Research Institute, Special Dispatch No. 1284.Middle East Media Research Institute (MEMRI). https://www.memri.org/reports/egyptian-regime-approves-church-construction-law-satisfying-coptic-church-interfaith
29. MERIP. (2011). Egypt and the Arab Spring: Sectarian politics and protest. Middle East Report, 258, 2–8.
30. Menza, M. F. (2021). *Citizenship and religious freedoms in post-revolutionary Egypt*. Religions, 12(7). https://doi.org/10.3390/rel12070516.
31. New Middle East. (2016). Church building and repair under Egyptian law. Retrieved from https://www.newmiddleeast.net
32. New Yorker. (2011). Egypt bombing: Alexandria church attack. The New Yorker, January 2, 2011.
33. Pennington, J. D. (1982). The Copts in modern Egypt. Middle Eastern Studies, 18(2), 158–179.
34. Canadian Coptic Human Rights Forum (CLHRF). (1999, December 12). *Press release on attacks against Copts in al-Kosheh*.
35. Tadros, M. R. I., El-Fiki, M. A., & Soliman, S. S. (1996). *The Copts of Egypt*. Minority Rights Group International
36. Tadros, M. (2009). Vicissitudes in the entente between the Coptic Orthodox Church and the state in Egypt (1952–2007). International Journal of Middle East Studies, 41(2), 269–287.
37. TIMEP. (2021). The contested politics of Coptic diasporic activism. *Tahrir Institute for Middle East Policy*.
38. TIMEP. (2021). The Coptic issue in Egypt: Developments and advocacy. Tahrir Institute for Middle East Policy.
39. U.S. Department of State. (2001). International religious freedom report: Egypt. Washington, DC: U.S. Government Printing Office.
40. U.S. Department of State. (2005). *Country reports on human rights practices—Egypt*. Bureau of Democracy, Human Rights, and Labor.
41. Vatikiotis, P. J. (1991). The history of modern Egypt: From Muhammad Ali to Mubarak (4th ed.). Baltimore, MD: Johns Hopkins University Press.
42. Wasef, Y. M. (2022). *Coptic diaspora activism and its impact on Egypt's religious policies*. *Journal of Middle Eastern Studies, 54*(2), 112–130. https://doi.org/10.1080/00263206.2022.2045678.

43. Wickham, C. R. (2002). Mobilizing Islam: Religion, activism, and political change in Egypt. New York, NY: Columbia University Press.
44. Wright, R. (1984). The politics of Egypt: State–society relations under Nasser and Sadat. Berkeley, CA: University of California Press.
45. WWRN. (2005). Egypt: Mubarak eases church repair restrictions. WorldWide Religious News.
46. Yefet, B. (2017). The Coptic diaspora and the status of the Coptic minority in Egypt. *Journal of Ethnic and Migration Studies, 43*(7), 1205–1221.
47. Zeitoun, S. (2012). Activism in the Coptic diaspora: A brief introduction. *Jadaliyya*.

Contents

Robotic warfare, Space, Cybercrime

Technological transformation, Green taxes

Shadow Warriors, Middle East