

AI and War

Hannes Werthner
Digital Humanism Summer School
Vienna, July 2026

Preliminary Remarks

- Based Michele Banfi, Wenhao Wu (Politecnico Milano, Italy), Dario Guarascio (University Sapienza, Rome), and Franco Accordino & Monika Lanzenberger (EC) and Web / AI search
- History of IT / Computer Science: close ties to military / war: ENIAC, Z3, Colossus, Microelectronics, Internet
- Game theory, Operations Research
- Public / Government Research and Technology Policy, see Vennavar Bush / MIT with the “linear roadmap” from basic research to innovation and growth
- A sensitive topic, in Digital Humanism and also in Academia (dual-use)
- **War** (von Clausewitz): continuation of politics by other means, never an isolated act of violence, but a tool used by nations to force an enemy to fulfill their will
Hard to delimit, when and where does it start and end.
- AI

AI on the Battlefield: A Reality



A smoke plume erupts over Khan Yunis from Rafah in the southern Gaza strip during Israeli bombardment on Jan. 8, 2024. Said KHATIB—AFP/Getty Images

Israel is using AI-powered airstrikes in Gaza to track and attack enemies



Robots don't bleed: Ukraine is sending machines instead of soldiers



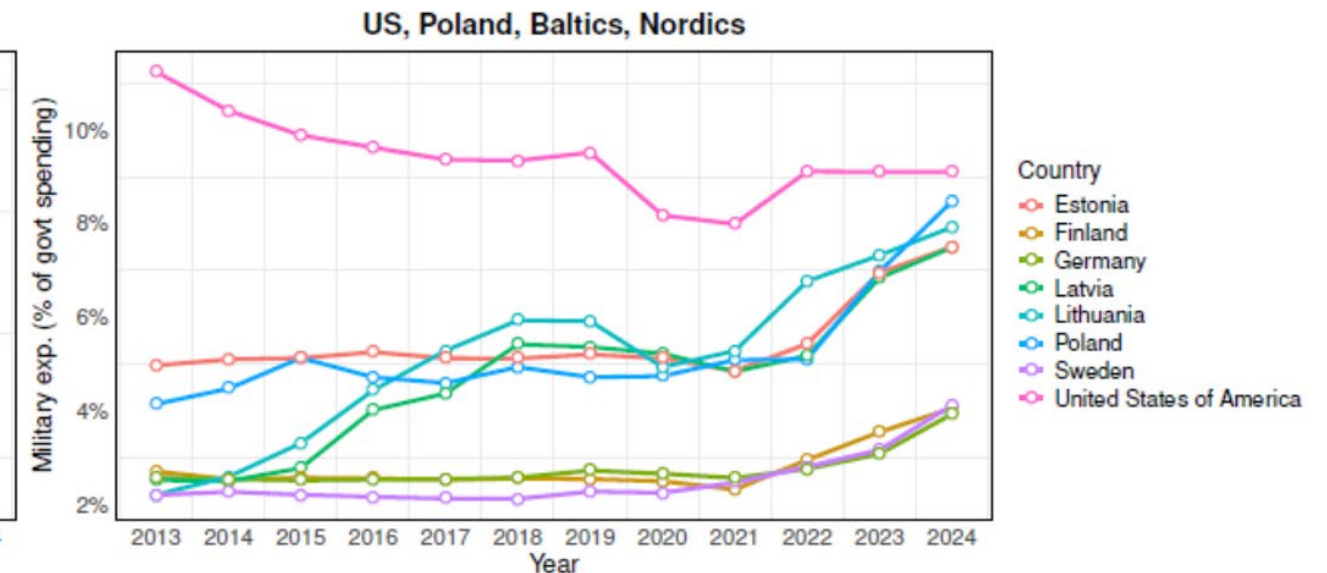
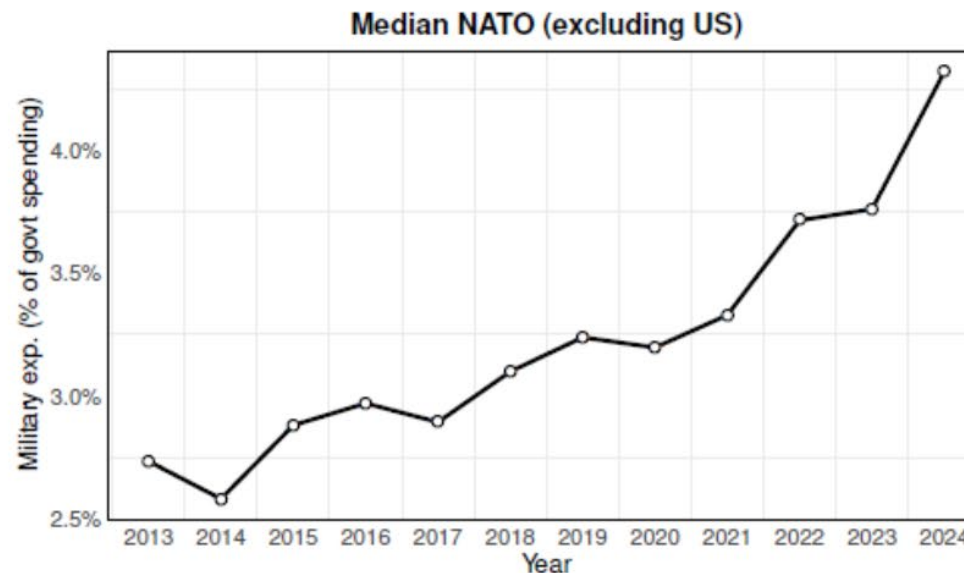
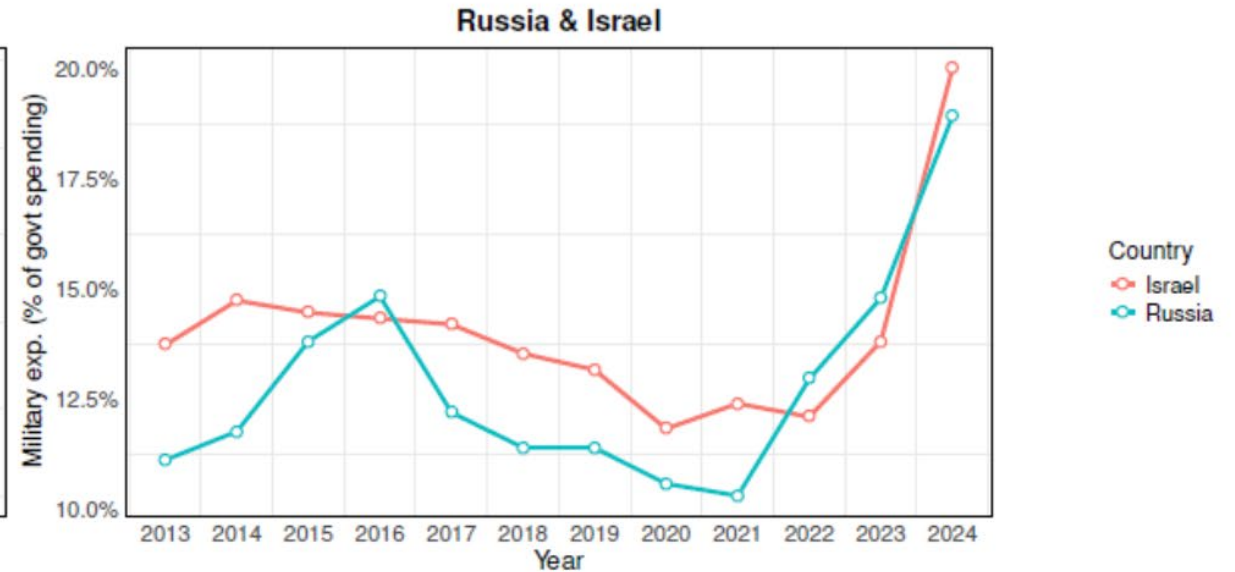
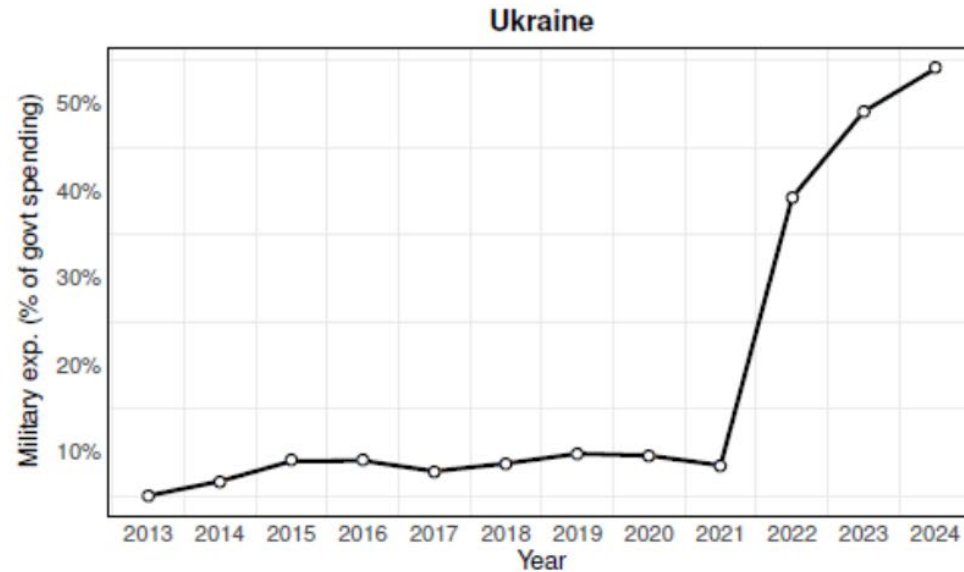
U.S. Big Tech support the US and Israel by providing ICT services and infrastructure

Background

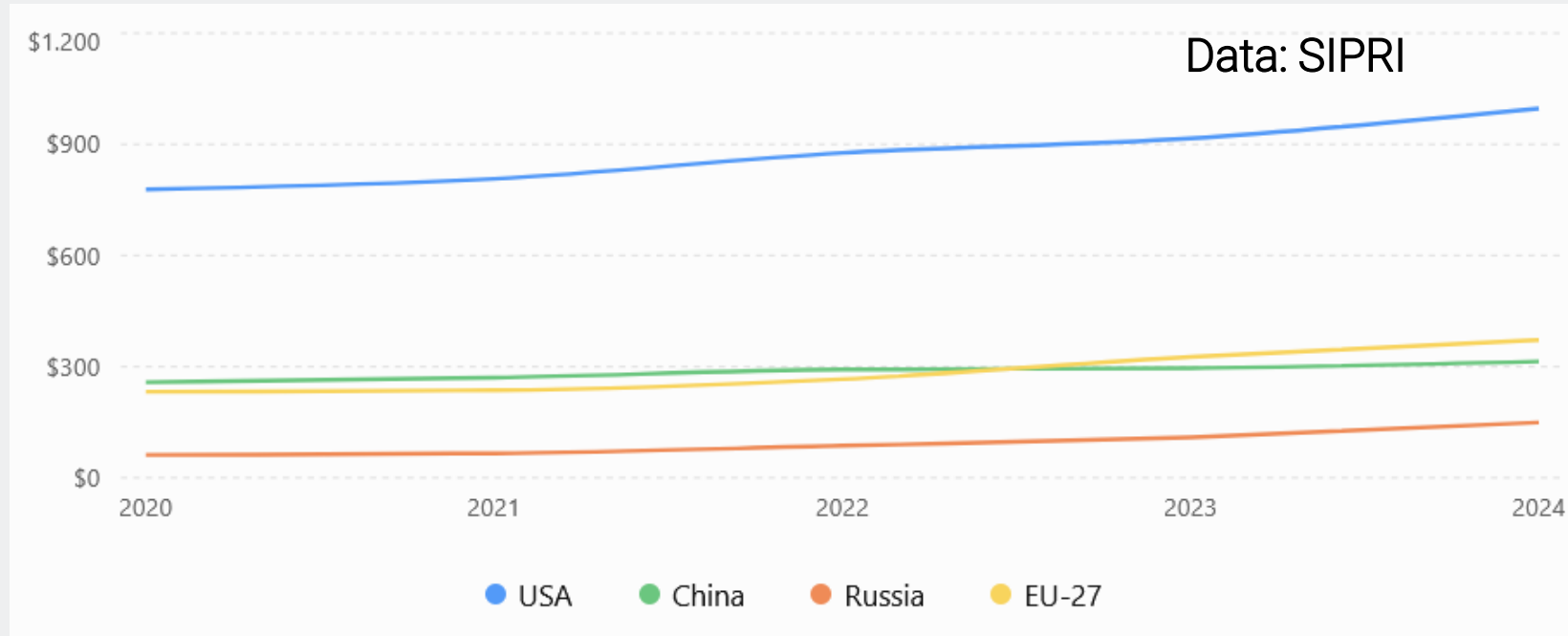
- From “end of history” (Fukuyama, 1992) with globalization to a new (dis)order in a multipolar world (not only geopolitics, also financial crisis and COVID)
- Decline in globalization, 35% decline in FDI
- Growing conflict between different power poles (incl military-digital complexes)
 - It’s about control over markets, technologies, and critical raw materials
 - *The return of imperialism (now expanded to include the digital sphere)?*
- Increase in military spending and the nuclear arms race
- Platform economy and surveillance capitalism (both growing)
- Rapid development of AI and its now-successful integration into robotics
 - *AI policy will be the most important issue in the 2028 U.S. presidential election* (Chris McGuire)

A new warfare regime?

Military spending, as a percentage of total government spending



Military Spending – a Comparison



Economic burden (% of GDP)

- United States: ~3.1% of GDP
- China: ~1.7% of GDP
- Russia: ~7.5% of GDP
- European Union: ~2.0 % of GDP

On 2024 total worldwide military expenditure \$ **2.718** trillion
9.4% increase from 2023 (largest increase since Cold War)
Equivalent to 2.5% of global GDP

Last Comparison: Cost to "Solve" World Hunger (yearly)

Baseline Target ~\$ **93** bn emergency & immediate support
Structural ~\$ **265** bn systemic changes

ICT: Developments in the Military vs. Civilian Sectors

- From the 1950s: important role of military procurement (first spende), for aerospace ("Sputnik shock" and the Vietnam War), and public R&D funding ARPA
- 1970s: declining costs for chips, electronics, and communication technologies due to growing commercial markets and also military spending
- Star Wars and thus indirectly the breakup of the Soviet bloc

- In the civilian sector, development of the platform economy and the commodification of services, virtualization, and network effects with "winner-takes-all"
- Market capitalization of Big Tech – economically and politically powerful

Convergence: Big Tech and ‘digitalization of war’

- Digital technologies important in military strategies
- Today increasing. see the U.S.-China rivalry in the field of AI
 - Important in the development and consolidation of the global technology hierarchy
 - Important in current and future weapons systems
- Military priorities and procurement a rapidly growing area for Big Tech companies (with likely implications for technological development)
 - E.g., focus on surveillance, remote-control, and autonomous systems

Political Economy of the the military-digital complex

- *Interdependence*:
 - The government cannot do without Big Tech in both, civilian or military sectors (economic scale, infrastructure, technologies, specific capabilities)
 - Big Tech needs government to secure its market share, prevent “hostile” regulations, and obtain public resources
- *Involvement in wars* (Ukraine, Gaza, Iran) provides technology companies with opportunities to develop and test new technologies and to strengthen their role within the military-industrial complex
- *Redesign of the old military-industrial complex* (Eisenhower): Technology transfer from the civilian to the military sector gaining importance (see the discussion at AI / Anthropic) and is changing public procurement processes
- *Important role of Big Tech* (along with “surveillance” companies, e.g., Palantir) in mobilizing knowledge, innovation, and public opinion

Why is IT (esp. AI) so important to the military?

- **Decision-making (DoD, 2024)**
 - Area of operations assessment and understanding
 - Adaptive force planning and its deployment
 - Rapid, precise, and resilient attack logistics and chains
 - Resilient logistical support
 - Efficient organization-wide processes
- **Autonomous weapons**
 - Drones, robots
 - AI-powered conventional weapons
- **Surveillance, Space, and Cyberwarfare (Coveri et al., 2024)**
 - Satellite and surveillance technologies
 - Carrying out and countering cyberattacks
- **System integration (virtual and physical)**
 - Establish / provide „digital platform“

AI on physical layer – “Kill-Chain”

- Improvements in information collection and decision-making
 - **Detect & Locate:** AI processes satellite and sensor data to automatically identify targets
 - **Track:** Predicts target movement patterns
 - **Aim:** The system recommends weapons and timing
 - **Attack:** "Autonomous" systems conduct attacks with minimal (or no) human intervention
 - **Evaluate:** The AI analyzes success/damage (in real time)

IT / AI in “Cyberspace” – in the virtual world

- **Weaponization** of the Web
- Warfare in the “cognitive” domain.
- Goal: influence opponent’s decision-making and public opinion
 - Automating real-time stories and social media interactions
 - Creating “false” credibility (e.g., deepfakes)
 - Cognitive biases (e.g., polarization dynamics)
 - Offensive operations (cyberattacks)
 - Supporting defense through reverse engineering (e.g., detecting anomalies in networks, identifying coordinated deception tactics)

IT / AI as Key in Geopolitics

- Besides its role for economic development
- Dependence on services (e.g., app stores for mobile services, cloud infrastructure)
- Denial of access, e.g., Anthropic and its models (Mythos and Fable)
- Preferred data access or denial of access (US Cloud Act)
- *Digital colonialism*

„Case“ USA

- Digital Platforms as the Government's *Eyes and Earsh*
- At home: companies are important to intelligence agencies and law enforcement
 - E.g. Microsoft provides threat analyses and reports on cyberattacks for the U.S. government
 - Palantir's Role at ICE
- Abroad: Support for intelligence agencies and military forces
 - Access to the cloud and prevention of access to digital services (Intern. Court of Justice, U.S. Cloud Act)
- Digitization of the defense budget: US government spending on digital military technologies is increasing rapidly and reached nearly \$100 bn in 2024.
- "Revolving doors" between the military and Big Tech
 - From Big Tech to government to utilize know how and networks
 - From military to Big Tech for "connections"
 - Former Apple Vice President (Doug Beck)
 - Former Alphabet CEO (Eric Schmidt)

China

- Only digital “ecosystem” comparable to the US
- Chinese Big Tech: Alibaba, Baidu, Huawei, Tencent
- Central to planning and industrial policy, and a policy of selective openness
- *Big Tech and the State/Party. interdependence* (systemic nature of "Big Tech", key role in promoting China's economic and technological growth, regulation as a factor)
- Companies control key infrastructure and technologies (semiconductors and AI) and also support the Party (e.g., the digital Belt and Road Initiative/fiber optic cables, data centers, smart cities, etc.).
- Increasing number of *joint ventures between Big Tech and the military.*
- Institutionalization of the military-digital complex and "revolving door effect": China's defense (focus on AI, satellites, and autonomous weapons), CEOs on CCP committees.

Europe

- Massive expansion of military budgets and increasing influence of the military complex (on politics and the public)
 - Hopes for growth effects
- “Caught” between the two military-digital complexes (sanctions, export bans)
- Europe's weakness in the digital world
- Militarization will likely lead to further dependence on the US (and also China)
 - In 2022, around 78% of European arms procurement came from outside the EU; the US accounted for approx. 63%. Planned decline to 20-40% is expected by 2030.
 - Higher in the digital sector: dependence in *cloud, infrastructure*, systems forming the *digital backbone* of many European *air forces* U.S. software share 100%; *battlefield AI* (U.S. companies such as Palantir, SpaceX)
- The European Move: Goal of IT and Data Sovereignty
 - European Defence AI Data Space (EDAIDS): data platform by 2030.
 - The “ReArm Europe” Program: Billions in AI, quantum computing, and drone startups via the European Defence Fund (EDF)
 - EU Tech Sovereignty Package

Big Tech go to war: Ukraine, Gaza and Iran

Keyrole in (digital) battlefield - „*brain*“ of war

Ukraine

- Microsoft: Shared cyber threat information with the Ukrainian military.
- Amazon: Migrated Ukraine's IT infrastructure to its cloud data centers across Europe.
- SpaceX: Deployed Starlink satellites to maintain critical communication links.

Gaza

- Google, Amazon, and Microsoft cloud computing and AI; Palantir analytics for military operations
- Israel uses AI systems to autonomously identify and prioritize thousands of targets

Iran

- Cloud-Infrastructure: Project Nimbus (Google & Amazon) / but employee protests
- AI for target identification and data analysis: US software and Israeli military algorithms for attacks on Iranian drone factories, nuclear facilities and military bases.
Palantir: integrates data from satellites, drones, communication and social media.
- Satellite communication and real-time analysis: SpaceX and companies like Maxar or Planet Labs
- Cyber defense and electronic warfare: Companies like MS, Google, Cisco with the NSA



And now Drones and Robots

- Term "drone" first used in the 1930s by the British RAF for unmanned aircraft. Unfortunate choice: drones are the only bees that don't have a sting.
- Enormous price reduction (high tech for the poor or even democratization?)

1. Transparent battlefield

2. **Asymmetry** (cost-benefit ratio): Weapon of few € destroy high-tech system of Mio €

3. **Fusion of sensor and weapon**: Drones may have cameras and also carry ammunition

4. **Protection of own personnel**: One would only lose plastic, batteries, and microchips.

5. **Integrated software/AI support**: Autonomous target recognition, swarm intelligence

6. **Less effort and personnel**: In the 2003 Iraq war, 2,000 military personnel needed to select 20,000 targets; in 2020, only 20.

“revolutionized” warfare, cheaper, more precise, more integrated, faster and more ruthless.

Technology

- Real-time sensing – Connected to ground and satellites -> Infrastructure and overall system
- Military platform
- Autonomous decision-making (also distributed / incl swarm)
- **Convergence of technologies**
 - AI
 - 5G / 6G
 - Edge / Cloud
 - IoT
 - Robotics
- Not only military use – Dual Use

Degree of Autonomy

- Most weapon drones used today are not fully autonomous.
 - Usually a human who makes important decisions, especially authorizing an attack
1. Remotely controlled drones
 - A human directly controls the drone.
 - Examples include many reconnaissance and combat drones..
 2. Semi-autonomous systems
 - The drone can navigate independently, avoid obstacles, or track targets.
 - Decision to use weapons rests with a human.(„human in the loop“).
 3. Fully autonomous weapon systems
 - System can autonomously identify, select, and attack targets without human authorization.
 - Such systems are technologically feasible to some extent, but politically and ethically controversial..

Flight Range, Armament, and Cost

- Depending on the mission:
- Range (up to over 2,000 km)
- Equipped with warheads and missiles (mostly expendable)
- Costs from a few thousand euros to millions of euros

Costs increase due to:

- Sensors and cameras
- Satellite communication
- Reusability
- Weapons carrying capacity
- Protection against electronic interference

- Large drone can cost more than hundred times as a simple kamikaze drone

- A commercially available FPV (First-Person-View) drone, modified for warfare and costing €500, and equipped with a Panzerfaust grenade, can destroy tanks worth €8-10 million.



Student work for a few thousand euros

Master thesis University of Västerås



- Ukraine (in particular) has been a development lab since 2022, producing from small reconnaissance drones to long-range attack drones.
- Not only on a few expensive systems but also on producing very large quantities of inexpensive drones.
Costs range from a few hundred euros to several hundred thousand.
- China, USA, Israel, Turkey, Iran, Russia, Ukraine most important exporters of military drones
- Global drone market is one of the fastest-growing sectors of the defense industry.

SUPPLY: CHINA'S STRUCTURAL DOMINANCE



Combat robots

1. *Small reconnaissance and demolition robots* (kamikaze ground drones): deployed en masse in Ukraine to lay mines, transport explosives, and

Armament/Function: Integrated explosives (kamikaze), mine-laying equipment, or cameras.

Cost: ~ €2,000 to €15,000 each.

2. *Infantry support and logistics robots*: tracked/wheeled; accompany soldiers on foot; transport heavy equipment, evacuate the wounded, or secure positions.

Armament/function: machine guns, grenade launchers, transport platforms.

Cost: from 30,000 to 350,000

3. *Heavy unmanned battle tanks*: weighing several tons / tracked. Designed to break through frontline defenses without risking the lives of a tank crew.

Armament/Function: autocannons, anti-tank missiles, or flamethrower rockets.

Cost: High-tech battle platforms of this size often cost between €1.5 and €3 million.



Combat robots – 2



4. *Walking robots* (robot dogs): advantage of being able to move over rubble, stairs, and rough terrain where wheels and tracks fail.

Armament/Function: Reconnaissance sensors, cyber defense, also equipped with assault rifles.

Cost: €100,000 to €250,000.

5. *Stationary autonomous watchtowers*: automatically monitor fixed defense installations, borders, and military bases.

Armament/Function: radar, thermal imaging cameras, machine guns.

Cost: €200,000+

- Trend: Moving away from expensive, highly complex pieces to modular systems under €500,000
- Goal: Large volumes so that the loss of a machine is financially and logistically manageable
- System networking / integration of drones, robots, infrastructure and conventional weapons, as well as swarm intelligence

What's wrong with that??

If not war altogether

- Loss of accountability
 - Unclear responsibilities for flawed decisions, mistaken attacks
- AI "flattery"
 - AI tends to reinforce users opinion
- Systemic bias
- Black-box decision-making and delegation of power
 - Humans become mere "yes-men" / just approve AI proposals
 - Decision is transferred to machines
- Drastically reduced time frame for human intervention (think of nuclear weapons)
- Becomes much easier to go to war
- In summary: increased risk of ...

International Response

- UN Secretary-General António Guterres called for a legally binding treaty to prohibit and regulate Lethal Autonomous Weapons Systems (LAWS).
- "Two-tiered" approach:
 - banning weapons that operate without human oversight,
 - strictly regulating all other autonomous systems to ensure meaningful human control.
- Status
 - More than 120 countries strongly support this, incl a preemptive ban.
 - Austria has been one of the leading nations at the UN.
 - Resistance by a minority oppose a global pre-emptive ban, prefer responsible military use and human responsibility
 - US, UK, Russia Israel, South Korea, North Korea, India, Japan, Australia, Poland, Belarus, Estonia – partly China

Conclusions

- “Automatization” of war
- Asymmetry of high-tech and cheap-tech (rich <-> poor)
- Growing escalation risks (e.g., through AI, including in the nuclear sector)
- Militarization of the IT sector, public discourse, and industrial/innovation policy
- The military-digital complex fuels conflicts and profits from them
- Cyber-physical convergence (drones, robots, infrastructure, satellites, swarm intelligence, conventional weapons) -> platforms
- Importance of knowledge and research
- Problem of universities with dual-use programs (especially in Europe, e.g., Germany (Civil Clause))

Conclusions

- Is the traditional military-industrial complex transforming into a military-digital platform complex, with the “Big Tech” as the new central (infrastructure) power?
- Does the line between civilian infrastructure and military systems disappear, including surveillance systems?

Conclusions

- The growth of the military-industrial complex has become a defining feature of the current political landscape and has become a key sector in the economy of various countries.
- The close link between economic interests, the military apparatus and political decisions produces an “armed nation,” in which war appears as a natural extension of politics, and the arms market becomes an autonomous driving force behind military decisions.
- Nor can we ignore the enormous economic interests behind war.
- The armaments industry, and countries that supply weapons, profit from a market that thrives precisely on conflicts. In this sense, there are also financial interests that contribute to fueling tensions in various regions of the world.

Author?