Next semester

I will add Odelya Natan soon, she may join our little group.... I guess next semester I will propose a reading course on these matters as a "policy observatory" where we read documents and reactions in media/social media to systematically monitor, analyze, and evaluate the policies within a specific domain... We could also establish an online presence and write small summaries etc. to check what impact such research has and get some interaction with the outside world even now (I can also design some agents that gather news and reactions to automatize this)... guess I could integrate this as part of the AI agents course. One important perspective that maybe interesting for Hila is this "costly signals" theory (actually originated in Israel and Noam has some related work on this), I'm for some reason ambiguous about this, something irritates me about it but it is rather influential, check this work https://cset.georgetown.edu/publication/decoding-intentions/ this is the media representation of that https://thebulletin.org/2023/12/costly-signaling-how-highlighting-intent-can-help-governments-avoid-dangerous-ai-miscalculations/ - so I'm not certain how many of these US executive orders fall into this category... but it is worth of having this theoretical lense... ultimately I'm not certain if this laters action is about strengthening alliances, diplomatic signaling, economic partnership, deterrence, it would be nice to capture all the perspectives first (does it shape trade agreements, international coalitions, or security alignments or maybe something else we don't see yet)

Possible Topics:

Framework for Artificial Intelligence Diffusion (IFR 0694-AJ90) is the first document that explicitly limits access to high-performance AI training hardware for certain countries and entities on the ground of national/strategy interest not because it wants to save humanity

etc…AI is becoming an extension of U.S. foreign policy and it is framed as a strategic instrument of power, similar to nuclear technology or the internet. Export controls on AI serve as a diplomatic tool, providing access to allies while limiting adversaries' technological capabilities

So for me it is fascinating how we switched so fast from all these global regulatory efforts to save humanity etc. to this cold war style regulation… does it say something about maturing of the technology or the geopolitical issues or the Silicon Valley bro fantasies of AGI caused it?

AI **is no longer just a regulatory issue—it has become a strategic statecraft issue**.

- **If AI were only about ethics and safety**, we would see **more international cooperation** and **binding treaties**. Instead, we see **military-style containment strategies** and **economic warfare tactics**.
- **If AI were just about technological maturity**, the focus would be on **open knowledge-sharing**, not **restricting model weights and compute power**.
- **If AGI were truly near**, governments would be **collaborating globally to prepare for its societal disruptions**—but instead, they are **competing to monopolize access** to AI capabilities.

This shift suggests that **AI regulation is now a function of power and control**, more than risk mitigation. The **promise of AI as a tool for humanity has been overtaken by its role as a battleground for geopolitical dominance**. Does this mirror broader historical trends, where technological optimism often collapses into power struggles once the stakes become clear?

Signs of this:

Export controls on AI chips and models indicate that AI is no longer seen as a neutral technology but as a **strategic tool for state power**.

The **U.S. has shifted from "saving humanity" with AI alignment talks to AI as a weapon of power**—something **to be controlled, denied to adversaries, and selectively shared with allies**.

The rise of **China's AI-powered surveillance state** has made the West more defensive, reinforcing the **AI nationalism narrative**.

In this framing, **AI governance is no longer about ethical use but about control,** who gets to have AI, and who doesn't. The **Cold War-style AI regulations** are more about **ensuring the U.S. remains the dominant AI power** than about global safety.

I'm actually worried this is all influenced by Silicon Valley's AGI Fantasies, the narrative pushed by Silicon Valley's most powerful AI labs, particularly OpenAI, Anthropic, and DeepMind.

- Advocate **AGI (Artificial General Intelligence) as an inevitable near-future event**.
- Frame AI **not just as an advanced tool, but as an existential force** that must be controlled.
- Have **direct ties to U.S. national security circles** and helped shape policy narratives about **AI "frontiers" needing government protection**.

This narrative benefits them in several ways:

- It **creates artificial scarcity**—by emphasizing **AGI danger**, they justify **closing models, centralizing power**, and **limiting open research**.
- It **aligns their commercial interests with U.S. security interests**, ensuring they receive funding, contracts, and influence over AI governance.
- It allows them to **dictate AI safety standards globally**, rather than allowing decentralized or public-sector control over AI.

By exaggerating the **speed and power of AGI**, they have helped push **governments into an arms-race mentality**, accelerating the shift from **global regulation to militarized AI control**.

Strange concepts in the document

AI diffusion

AI as a national/strategic asset - sociotechnical imaginary of AI as a 'controlled resource'
AI is increasingly treated like nuclear technology or strategic natural resources, requiring international monitoring, security protocols, and containment. What are the exact fears? How this differs from AGI/ASI… AI is becoming a regulated commodity that must be strategically controlled to maintain U.S. leadership in the field, how will other actors react? What is this actor-network in making? It is not just a software, but a critical infrastructure, requiring secure data centers, controlled export policies, and compliance with global cybersecurity measures.

AI Model Weights More Critical Than Code (Controlled Export Item)

Surprisingly, AI model weights the numerical parameters trained through vast computational power. are now classified as export-controlled items under the Export Administration Regulations (EAR). This is because controlling access to model weights is seen as the most effective way to prevent adversaries from leveraging AI for harmful purposes. The document asserts that while AI architectures and training code can often be replicated or reverse-engineered, the model weights are the most valuable and difficult-to-reproduce aspect of an AI model. As such, controlling the distribution of model weights is deemed crucial to maintaining technological superiority.

Foreign Direct Product Rule (FDPR) for AI Models

AI as a National Security Risk and Strategic Asset

The document emphasizes that AI is no longer just a technology but a strategic geopolitical asset. It argues that AI can be used to enhance national security but also poses extreme risks, including facilitating the development of weapons of mass destruction (WMDs), cyber warfare, and human rights abuses through mass surveillance

AI as a New Strategic Resource: Governing Technological Diffusion?

Explore how and why is AI being framed as a critical national security asset, shaping governance strategies and international tensions?
How do governments define AI as a strategic resource, and how does this classification shape export controls and international trade policies?
What are the historical precedents for controlling the spread of a foundational technology, and how do AI regulations compare to previous cases like nuclear technology, cryptography, and aerospace?
How do AI governance frameworks reflect shifting attitudes toward national security and economic protectionism?

Maybe with a focus on Israel?
Given Israel's strong semiconductor and AI sector, examine how the country is maneuvering between U.S. regulatory pressures and economic opportunities with China?

How is the Israeli government balancing its relationship with the U.S. and its growing tech ties with China?
What role does the Knesset and various committees play in shaping Israel's response to U.S. export controls on semiconductors and AI?
How do Israeli technology firms adapt to an increasingly polarized global technology landscape?

Geopolitical Spectacle of AI Governance

AI chips reflect deeper anxieties about human agency, control, and geopolitical power. The research would connect Cold War technological imaginaries to contemporary AI governance, showing how regulatory actions are as much about ideological myth-making as they are about practical security concerns.

How do contemporary AI governance debates reflect historical patterns of technological fascination and fear, as seen in Cold War-era narratives?
In what ways is AI constructed as both a utopian and dystopian object in policy discourse, shaping export controls, national security concerns, and economic competition?

How does the dual perception of AI as an existential threat and an economic boon inform state strategies and regulatory frameworks?

ASI: From AI Super Intelligence to AI Supremacy?

- AI as the new "Sputnik moment" for national security and economic competitiveness.
- Narratives of AI-driven progress, from automation to artificial general intelligence (AGI).
- The role of AI in national myth-making, mirroring past admiration for nuclear energy, space exploration, and the internet.
- AI as an uncontrollable, self-propagating force - Cold War anxieties around nuclear proliferation.
- The weaponization of AI fears in policy documents (AI as a tool for authoritarian surveillance, disinformation, and warfare).
- The specter of China as an AI "boogeyman" in U.S. policy, fueling restrictions similar to past embargoes on Soviet computing.
- The fantasy of AI as a sovereign asset, much like oil or nuclear weapons, despite its reliance on globalized supply chains.

From MAD to AI: The Geopolitics of Technological Containment

The New Tech Cold Ward: Export Controls as Political Alliances

Explore the parallels between Cold War deterrence strategies and current AI containment policies, questioning whether AI diffusion is a new form of strategic arms race.

- How do recent U.S. semiconductor restrictions compare to Cold War-era technology embargoes, such as CoCom (Coordinating Committee for Multilateral Export Controls)?
- To what extent do current U.S. export controls signal the decline of globalization and the rise of regionalized technological ecosystems?
- How are China and other affected nations developing counterstrategies to maintain access to restricted technologies?
- How does the U.S. semiconductor strategy compare to Cold War nuclear arms control in terms of containment and deterrence?
- How do U.S. export controls on semiconductors resemble past Cold War strategic denial policies, such as the restrictions on Soviet access to advanced computing in the 1980s?
- What are the risks of AI diffusion into geopolitical adversaries, and how does this compare to nuclear technology proliferation?
- How do technology transfer policies reflect a shift in strategic thinking from Mutually Assured Destruction (MAD) to AI and computational dominance?

CoCom (Coordinating Committee for Multilateral Export Controls) (1949–1994): A U.S.-led export control regime restricting advanced technologies to the USSR and its allies.
National Security Directives: The U.S. tightly controlled semiconductor, aerospace, and computing exports, fearing “technology leakage” to Soviet military programs.
Industrial Espionage & Counterintelligence: Both sides conducted extensive espionage (e.g., Soviet theft of IBM mainframe designs) while also employing counterintelligence to protect industrial secrets.

Links to the materials:

https://www.bis.gov/press-release/biden-harris-administration-announces-regulatory-framework-responsible-diffusion

https://www.bis.doc.gov/index.php/regulations/federal-register-notices#90frxxx

https://www.bis.doc.gov/index.php/licensing/validated-end-user-program

https://www.bis.gov/press-release/commerce-strengthens-restrictions-advanced-computing-semiconductors-semiconductor

https://www.federalregister.gov/documents/2025/01/16/2025-00480/additions-to-the-entity-list

https://www.bis.gov/press-release/commerce-strengthens-restrictions-advanced-computing-semiconductors-semiconductor

https://www.bis.doc.gov/index.php/regulations/federal-register-notices#90frxxx

https://www.bis.doc.gov/index.php/documents/federal-register-notices-1/3563-90-fr-4544-framework-for-artificial-intelligence-diffusion-ifr-0694-aj90-1-15-2025/file

https://www.tomshardware.com/tech-industry/eu-preps-chips-act-2-0-to-stregthen-semiconductor-industry-after-original-program-reportedly-flopped

Reactions:

https://blogs.nvidia.com/blog/ai-policy/

https://main.knesset.gov.il/en/news/pressreleases/pages/press15125q.aspx