From Hacking Systems to Hacking Humans: AI, Weaponized OSINT, and the Rise of Personal Cognitive Defense

Sohith Vishnu Sai Yachamaneni
University of Zürich
Submitted for Seminar: AI, Politics, Society: A Critic

February 18, 2026

1 Introduction

Let me introduce a scenario: In the current world, everyone is very active in the digital space. An individual has a large public digital footprint because we live in a digital society nowadays. From LinkedIn profiles for networking in formal ways, to Facebook, Instagram, and X for informal connectivity, and public review histories on Amazon or forums like Reddit. The amount of data we are providing to open platforms ranges from individual sensitive information to opinions, which we share on the open internet for the public to see. For most people, these are fragmented, harmless pieces of public information that are intended for their own benefit or the benefit of others, as this is becoming more of a norm. People assume it's mandatory as they are pulled into the ecosystem of the digital lifestyle. Now, let's start with the following question: "Is there a way this information can affect me in any manner?" For individual pieces of information, it's a no, or maybe a slight off-chance. But to a human bad actor, this is good enough information to create a profile of you. But this is just the beginning because, with current advancements in Artificial Intelligence, this might change in a radical way. While a human can go through a couple of information points to try to guess a password, modern AI might create a Psychometric Profile by using the digital footprint that we build over the years.

Until now, human bad actors used this little information they could gather to trick users and pave a path for themselves. With a phishing email, for example, they try to analyze a large amount of people using a particular service on the internet; if they send a phishing email, they can phish some information randomly. If they have a target in mind, they have to gather intelligence on the person, tail them to find patterns, and take days or months to get a correlation. This takes planning, skill, and a thought process to carry out. Now, let's take away that planning, skill, and thought process needed to target a person to gather intelligence, and outsource it to an AI. A script-kiddie (in cybersecurity, a "script-kiddie" refers to a hacker who relies on pre-made scripts and programs to perform malicious actions, rather than creating their own. Calling someone a script-kiddie implies they only have surface-level knowledge of computer systems and are inexperienced) can rise to the level of a malicious hacker with little to no knowledge. Now, for an average person, detecting a phishing attack is hard. What if using a high level of sophisticated intelligence gathering and deepfakes can create a situation where they will oblige your request? Sounds scary and right out of science-fiction; unfortunately, we are closer to this reality than we thought.

In this exploratory paper, I am reviewing the risks of Weaponized OSINT (Open Source Intelligence) and how Data Deanonymization will change radically in the next couple of years, the risk towards general populous, Ethical Concerns, Legal Blind spots and Relection on the governance.

2 Weaponized OSINT and Data Deanonymization

Historically, **Open Source Intelligence (OSINT)** has been employed by academics and journalists as a means of promoting openness and scrutiny. However within the combined domain of Artificial Intelligence, Data, and Cybersecurity, OSINT acquires a distinctly hazardous dimension. Methods originally designed to surface public-interest information are now leveraged by adversaries to construct high-resolution target profiles. This evolution reflects a clear shift from observational data collection towards intentional and exploitative targeting

2.0.1 The Mechanism of Weaponized OSINT

"Weaponized OSINT" refers to the use of OSINT in the context of identifying human vulnerabilities through public sourced information. Recent Research [5] shows that attackers effectively gather "as much as information as possible" from the sources ranging from "online databses containing leaks to social media platforms". This process will take huge step with use of AI, this is allows for:

- **Automated Aggregation:** AI systems do not interpret information as isolated signals. Instead, they continuously collect and correlate large volumes of publicly available content—such as professional

profile changes, casual social media remarks, or images of personal workspaces—into a coherent and actionable profile [12].

- **Psychometric Inference:** Once aggregated, these disparate data sources enable the extraction of behavioral and personality indicators. At this stage, the attacker no longer engages with an abstract "user," but with a psychologically characterized individual—for example, someone demonstrably receptive to social validation or interpersonal engagement—which allows for highly tailored manipulation [12].

From an **organizational perspective**, publicly accessible information is similarly exploited to reconstruct internal structures and decision-making hierarchies. By isolating high-value roles—such as system administrators, finance executives, or their immediate support personnel—attackers can orchestrate precision attacks designed to evade broad, perimeter-based security defenses [12].

2.0.2 Deanonymization and The Mosaic Effect

One of the most severe data protection threats in this domain is deanonymization, often referred to as re-identification. This risk emerges when an adversary combines a dataset that has been deliberately anonymized—such as a publicly released health survey or aggregated customer feedback—with information available from open online sources. By correlating these datasets, the attacker can reconstruct the real-world identities of individuals originally believed to be protected.

This process is commonly explained through the concept known as the "Mosaic Effect." A single piece of information may appear insignificant in isolation; yet, when numerous such fragments are assembled, they collectively expose sensitive details about a person's identity, behavior, and circumstances. [11]

As a result, conventional anonymization measures prove increasingly fragile. When an individual maintains a distinctive public digital footprint, removing explicit identifiers from a dataset is no longer sufficient. Given enough auxiliary data and analytical capability, a modern AI system can reliably reverse anonymization and re-link the data to its original subject.

2.0.3 Existing Regulatory and Governance Landscape

In the Regulatory space there are FADP Art. 5 and Art. 30 and GDPR Article 9 has the protection over sensitive information and profiling. I am considering both references of the GDPR due to its doctrinal maturity and detailed treatment of the data processing and inference, as the Swiss Federal Act on Data Protection (revFADP), which aligns closely with GDPR principles has lead to the same blind spots largely persist and even offer fewer explicit safeguards regarding inferred data and public-data aggregation. While the revised Swiss FADP adopts the GDPR's doctrinal maturity in defining 'High-Risk Profiling' (Art. 5g) and 'Personal Data' (Art. 5a), it inherits the fatal 'Public Data Loophole' (Art. 30). Ultimately, the law fails not in its definitions, but in its enforcement which we discuss more in the Reflection on Governance

3 Weaponized OSINT and Data Deanonymization: Impact on Individuals and Corporations

With the foundation of Weaponized OSINT and Data Deanonymization, the transition from theoretical capabilities to practical impact shows us the effect within the general public and organizations. The benefactors (the General Public, Social Media Platforms or Data Reservoirs, Malicious Actors, and Independent Investigators) and victims are intertwined here. Depending on which edge of the sword you are on, you can either be a benefactor or a victim of this.

3.1 Weaponized OSINT and the General Public

In the public domain, the benefactors and victims form an asymmetric ecosystem, The General public often individuals living their digital lifestyle, their primary interest is convenience and social connection, often unaware of the privacy tradeoffs. The social platforms or Data Reservoirs, their business model relies on maximizing the engagement and data harvesting for targeted advertising. The Malicious actors ranges from unorganized script kiddies to state-sponsored actors, their interest ranges from financial extortion or ideological disruption. Independent Investigators OSINT practitioners who uses these tools for accountability and transparency.

3.1.1 Impact on the public: Harms, Risks, and Benefits

Hyper-Personalized Exploitation: Where the public faces severe risks from AI-precision attacks. AI can automates the scraping of digital footprints to build psychometric profiles. This will leads to manipulation: voice cloning, video spoofing (deepfakes) in real-time. For example, in one high-profile case a mother was manipulated into believing her daughter had been kidnapped after reviving a call with an AI-Cloned voice - testimony she later presented to the U.S. Senate Judiciary Committee to highlight the threat of such scams [10]. In another story which highlight how AI-powered deepfake and "nudify" apps are driving many Indian women to reduce or cease their online activity out of fear of manipulated images and extortion, demonstrating real-world social harm from generative AI misuse [9].

Cognitive Hacking and Consensus Manipulation: Beyond individual targeting, lets shift our perspective to a border view, in collective perspective the general public faces a severe collective threat: **Cognitive Hacking**[3]. In this context, public data is not just a resource to be harvested but a surface to be poisoned. Malicious actors utilize AI to inject synthetic data into the public discourse, effectively manipulating the "census of reality" to ideologically engineer specific demographics. This psychological manipulations will diminishes the trust in institution and amplifies social divisions, operating not by hacking computer systems, but by hacking human perceptions. For example: A group named "Australians for Natural Gas" presented itself as a grassroots citizen moment through target online group was actually orchestrated by a political party's internal pollster to artificially boost public support for the gas industry ahead of a federal election. Other groups with benign-sounding names like "Mums for Nuclear" and "Australians for Prosperity" similarly utilized digital ads to suggest organic grassroots concern while obscuring the deeper agendas of wealthy donors and coal interests[4]. Even though, the AI utilization is not mentioned, but the platforms these ads are running, targeting to them large users in selected manner which makes it in the scope of AI, a future prediction towards AI planned and thought out Astroturfing with the tools of OSINT in large consensus is something we have to worry about.

Despite the harms and risks, the democratization of OSINT retains immense value for the public good. Investigative networks use AI to collect and verify digital evidence from social media, exposing human rights violations and supporting criminal justice accountability. For example, Ukrainian Investigators in collaboration with over 45 NGOs, where able to identify around 50 potential perpetrators with AI and OSINT tools [6].

3.1.2 Power Imbalances, Conflicts and Missing Voices

The Power Dynamics: There is a severe power imbalance. Control over data currently rests entirely with the Data Reservoirs and AI Developers. They create the models and hold the data, leaving the general public completely defenseless against how their open internet history is scraped by LLMs. Unlike corporations with multi-million dollar defense budgets, the general public is relegated to a purely reactive state against advanced algorithmic manipulation. This means we can no longer trust "Public Sentiment" as a raw metric; decision-making based on unverified public data is now a critical societal vulnerability.

Conflicts of Interest: A fundamental conflict exists between Social Platforms (whose algorithms incentivize public data sharing and virality) and the General Public (who require privacy to prevent Deanonymization and AI profiling). Furthermore, open-source AI developers, who want to democratize access to AI for

innovation, inadvertently align with malicious actors by removing the skill barrier for launching sophisticated attacks.

Missing Voices: The elderly, the digitally illiterate, and the socioeconomically disadvantages are absent from the mainstream tech governance discussions. As, we are passing over from the digital firewall to human psychological firewall. Its need to educate on the current technological advancements to the missing voices.

3.2 Weaponized OSINT and Corporations

Unlike the public domain, the corporate domain is highly asymmetric. However, the financial stakes are significantly higher and they also interlinked with public domain, where these corporations contain information regarding public domain as well. But the corporate domain posses technical capabilities and defensive strategies compared public domain. Corporate employees and executives provide valuable insights through their digital footprints, helping organizations understand operational patterns. Security teams harness AI-driven OSINT to protect networks, safeguard intellectual property, and prevent financial losses. Open-source AI developers advance the field by creating tools that empower both defenders and analysts, while even threat actors, though malicious, inadvertently drive innovation by challenging security systems to evolve. Together, these actors illustrate how AI and information flow can enhance awareness, resilience, and efficiency across the corporate ecosystem.

3.2.1 Impact on the public: Harms, Risks, and Benefits

Deepfake Business Email Compromise: Corporations face a new era of highly intelligent social engineering. Malicious actors scrape information from Linked ln or any other networking sites, try to map out corporate hierarchic, vendor relationships and communication patterns. They then use AI to impersonate executives via audio or video, bypassing the standard identification protocols and manipulating employees into authorizing fraudulent wire transfers. For example: A finance worker at a multinational firm in Hong Kong was tricked into transferring 25 million dollars to scammers. The worker was manipulated during a live video call where deepfake technology was used to realistically impersonate his company's Chief Financial Officer and several other colleagues simultaneously. The employee believed he was in a routine financial authorization meeting [1].

Standing on the other edge of the sword, corporate security team utilize the exact same AI-driven OSINT capabilities for threat intelligence. Some companies uses some part of this ONIST and AI driven in their business model to appeal to the general consensus.

3.2.2 Power Imbalances, Conflicts and Missing Voices

The Power Dynamics: Unlike the general public, large corporations possess the budget to engage in an "AI Arms Race." By employing inference-based detection methods using multiple concurrent models, enterprises can analyze video and audio in real-time to detect AI signatures.

Conflicts of Interest: The conflict of the open-source AI developers, is also affects in the corporate domain. The democratization of these tools allows low-level criminals to launch high-level corporate scams that were previously restricted to state-sponsored actors.

Missing Voices: Small to Medium Enterprises (SMEs) are largely missing from the corporate AI conversation. While Fortune 500 companies dominate the narrative around AI defense, SMEs lack the resources to defend themselves. They are highly lucrative targets for scalable AI-phishing campaigns, yet their specific vulnerabilities are often overlooked in mainstream policy discussions.

4 Beyond the Black Box: Future Implications and the Crisis of Governance

As Weaponized OSINT transitions from theoretical capability to practical deployment, its impact exposes a fundamental disruption of the digital social contract. The implications of this shift extend beyond immediate financial loss, threatening the structural integrity of digital trust and democratic consensus. The current landscape of this technology is evolving so rapidly that traditional regulatory enforcement has become trivialized. We are entering an era where AI architecture allows developers to claim technical anonymity, while attackers launder their criminal liability behind the opacity of the algorithmic "Black Box."

4.1 Key Tensions, Ethical Concerns, and Legal Blind Spots

The problem of **"Public Data Paradox"**. The internet has been operated in the assumption that public data inherently benign. However, current legal and ethical frameworks have failed to keep pace with how modern tech transformation and how AI transforms this open data into exploitable intelligence.

- **The loophole (GDPR Art. 9 [7] Swiss FADP Art. 30 [2])**: The primary legal defense against Weaponized OSINT is the distinction between "Private" and "Public" data. The GDPR and Swiss FADP strictly prohibit the processing of sensitive data (like psychological traits or political opinions). However, this protection is redundant under the "manifestly made public" loophole. Attackers and AI data brokers abuse this loophole, arguing that because an individual Tweeted about a "stressful week" (public), the AI's inference of "High Neuroticism" (sensitive psychological data) is fair game [12].
- **The Ethical Concern (Contextual Integrity)**: This creates a blind spot where "Inferred Privacy" is left unprotected. It violates the principle of Contextual Integrity. Information shared in one context (a casual social post) is weaponized in a completely different context (a cyber-attack). De facto consent is inferred from public availability, despite the absence of express consent[12].
- **Asymmetry of Accountability and Victim Blaming**: When an AI-precision phishing attack succeeds, current frameworks view the human victim as "negligent." Organizations default to punishing or "retraining" employees. Ethically, this is flawed. If an AI uses super-human psychological profiling to bypass human cognition, punishing the human is similar to punishing a user for a firewall failure[12].

4.2 The Governance Gap: "On-Paper" Protection vs. Technical Impunity

While the legal guardrails that protects users exists on paper, they suffer from a fatal enforcement gap.

4.2.1 The Enforcement Scenario: The "Black Box" Dilemma

While the theoretical legal guardrails exist, applying them in a real-world scenario reveals a fatal flaw in the enforcement architecture. Consider a standard OSINT attack: an attacker uses a General Purpose LLM to aggregate public data and shadow-profile a specific Swiss citizen.

Legally, this triggers the FADP and GDPR. However, when law enforcement attempts to prosecute this crime, they face an impossible "Laundering of Liability" scenario:

- **The AI Developer is Shielded:** The authorities cannot prosecute the AI company. Because the developer trained the model on aggregated public data without specific individual identifiers, they have achieved "Anonymization" at the model level. They are legally immune from how the tool is subsequently used. But at the same the LLM might developed an Butterfly effect based learning from different sources could give raise to super profile which is an aggregation of all the anonymized data to aggregated consensus profile.
- **The Attacker Evades Detection:** The authorities must prosecute the attacker, who is now the legal "Data Controller" and liable for criminal fines under FADP Art. 60[2]. However, the attacker's act of "Group-to-Individual Inference" occurs entirely inside an encrypted, un-auditable LLM query—the

"Black Box" and the attackers, might give the reason that unawareness of the super-profile which might lead him to such conclusion.

Conclusion on Governance: There is no paper trail, no visible breach, and no way to audit the private AI query. Because law enforcement cannot see inside the Black Box, the attacker's criminal liability is effectively laundered. This scenario proves that traditional, top-down regulatory enforcement is functionally might be obsolete against AI-driven OSINT. To protect the public, governance must urgently shift toward individual empowerment and Personal Cognitive Defense.

4.3 Future Threat Trajectories and Societal Vulnerabilities

As this trend contentious in-terms of governance, the implications over the few years might be concerning towards, a **Rise of the "Zero-Turst" Human** it means no human trusted by default, as AI deepfakes and voice cloning reaching a level distinguishing them is practically impossible and layer of additional verification like 2-factor authentications to humans will be introduced. **Autonomous Botnets and The Truth Gap** as discussed perviously "Cognitive hacking" even with EU AI Act (Article 50) [8] mandates that AI-generated content be marked as such. However, this is technically unenforceable with text-based systems.

Vulnerable Groups: While corporate heists dominate the media, the true victims are the elderly and socioeconomically disadvantaged. They lack the digital literacy to spot AI signatures and the financial resilience to recover from losses. Furthermore, this creates a "Chilling Effect" on free expression, causing vulnerable populations to self-censor and retreat from the digital public square out of fear of AI exploitation.

4.4 Personal Cognitive Defense: Policy Guidelines for Individual Resilience

From my pervious work "How AI Transforms Fragmented Public Data into Targeted Cyber Threats" [12]. I have proposed a framework for personal cognitive defense. As the we are shifting from the System Security to Personal Cognitive defense.

- **Defensive Compartmentalization (Countering Weaponized OSINT)**: Attackers aggregate data from multiple sources to build a target profile. Users must enforce strict "Identity Segregation." Do not allow your Professional Persona (LinkedIn) and Private Persona (Instagram/X) to touch. Use different profile pictures and usernames. Maintain a "Boring Professional Rule"—by limiting emotional expression on professional channels, you deprive the AI of the data points it needs to profile you.
- **The "Affective Gap" Protocol (Countering AI Phishing)**: We typically treat "bad grammar" as a sign of a scam. In the AI era, we must treat "Emotional Urgency" as an Indicator of Compromise (IoC). If a digital message triggers a sudden spike in emotion—whether fear (Neuroticism) or a desire to help (Agreeableness)—you must effectively "pause" the interaction. Verify the sender through a secondary, non-digital channel. Trust the voice, not the text.
- **Active Data Sovereignty (Countering Shadow Profiling)**: Users must proactively utilize GDPR Article 15 (Right of Access) and Article 17 (Right to Erasure) to query and delete their shadow profiles held by data aggregators. Where erasure is impossible, users should adopt "Data Poisoning." Feeding conflicting or nonsensical data into the public web (e.g., browsing random products you do not need) can lower the confidence score of the AI trying to profile you, effectively masking your true psychological traits.

5 Conclusion

As we have explored, the convergence of OSINT and AI represents a structural shift in the scale of digital harm that can be produced. Public data, once assumed benign in isolation, can now be transformed into high-resolution psychometric intelligence, capable of enabling precision social engineering, deanonymization, and cognitive manipulation. This marks a definitive shift in the threat landscape: we have officially moved from an era of "Hacking Systems" to an era of "Hacking Humans."

The current governance landscape, while doctrinally mature on paper, might be functionally obsolete against this new reality. As demonstrated by the "Public Data Paradox" and the opacity of the algorithmic "Black Box," attackers can now operate with near-total impunity, laundering their liability while regulators remain blind. We can no longer rely on top-down institutional guardrails or the hope that social platforms will self-regulate against their own financial interests.

However, the solution is not going back to stone ages but advancement learning how to navigate this new digital space. Instead, the rise of AI-precision targeting necessitates the evolution of the "Human Firewall." Privacy is no longer merely about secrecy; it is about cognitive autonomy and control. By understanding how AI interprets our digital exhaust our openness, agreeableness, and neuroticism. we can construct a "Defensive Visibility." Adopting the principles of Personal Cognitive Defense allows us to participate in the digital ecosystem without becoming its casualty. Ultimately, defending against the future of Weaponized OSINT is not a matter of better code, but of better human awareness.

6 Declarations and AI Use Acknowledgment

Declaration of Prior Work / Self-Citation I hereby declare that this seminar paper, The Weaponization of Personality, builds upon foundational concepts and policy frameworks initially developed in my prior assessment: How AI Transforms Fragmented Public Data into Targeted Cyber Threats (submitted December 11, 2025).

To avoid self-plagiarism, direct overlap has been strictly limited to the necessary definitions of "Weaponized OSINT" and the "Personal Cognitive Defense" framework in Section 4.4 , which have been summarized and properly cited. This current paper expands the scope from technical attack mechanisms to a novel analysis of governance, stakeholder dynamics, and legal blind spots.

I acknowledge the use of **Google Gemini** (Large Language Model), published by Google (URL: https://gemini.google.com) to assist in the preparation of this assessment.

Specifically, I used the tool for the following purposes:

- **Ideation and Structuring:** To brainstorm the legal concepts of GDPR and FADP to create scenarios and better understand and used in structuring the paper to ensure its flow.
- **Polishing:** To contextualized certain text to fit the specific constraints of the assignment and remove mistakes.
- **Technical Formatting:** To generate the LaTeX code used for the document's layout and bibliography.
- **Alignment**: To make sure my writing style is aligned with what project should cover, rather than drifting into narrative storytelling

References

[1] Heather Chen and Kathleen Magramo. *Finance worker pays out $25 million after video call with deepfake 'chief financial officer'*. Accessed: 2026-01-24. CNN. Feb. 2024. URL: https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk.

[2] Swiss Confederation. *Federal Act on Data Protection (FADP) (AS 2022 491) (English translation)*. Accessed: 2026-01-24. Fedlex – The Federal Law Portal of Switzerland. Sept. 2022. URL: https://www.fedlex.admin.ch/eli/cc/2022/491/en.

[3] cyber-espionage. *Cognitive Hacking: Manipulating Perception, Influencing Decisions*. Accessed: 2026-01-23. URL: https://www.cyber-espionage.ch/Cognitive_Hacking.html.

[4] Daniel Angus, Christine Parker, Giselle Newton, Kate Clark, Mark Andrejevic. *What political ads are Australians seeing online? Astroturfing, fake grassroots groups, and outright falsehoods*. Accessed: 2026-01-23. Apr. 2025. URL: https://findanexpert.unimelb.edu.au/news/103230-what-political-ads-are-australians-seeing-online%3F-astroturfing--fake-grassroots-groups--and-outright-falsehoods.

[5] Sergiu Eftimie, Radu Moinescu, and Ciprian Răcuciu. "Spear-Phishing Susceptibility Stemming From Personality Traits". In: *IEEE Access* 10 (2022), pp. 73548–73561. DOI: 10.1109/ACCESS.2022.3190009.

[6] Olga Golovina. *Artificial Intelligence and War Crimes Investigations*. Accessed: 2026-01-23. Institute for War and Peace Reporting. Jan. 2024. URL: https://iwpr.net/global-voices/artificial-intelligence-and-war-crimes-investigations.

[7] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. EN. Official Journal of the European Union, L 119, pp. 1–88. Current consolidated version: 04/05/2016. ELI: http://data.europa.eu/eli/reg/2016/679/oj. May 2016.

[8] *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)*. EN. Official Journal of the European Union, L 2024/1689. In force. ELI: http://data.europa.eu/eli/reg/2024/1689/oj. July 2024.

[9] The Guardian. *'The chilling effect': how fear of 'nudify' apps and AI deepfakes is keeping Indian women off the internet*. Accessed: 2026-01-23. Nov. 2025. URL: https://www.theguardian.com/global-development/2025/nov/05/india-women-ai-deepfakes-internet-social-media-artificial-intelligence-nudify-extortion-abuse.

[10] The Guardian. *US mother gets call from 'kidnapped daughter' – but it's really an AI scam*. Accessed: 2026-01-23. June 2023. URL: https://www.theguardian.com/us-news/2023/jun/14/ai-kidnapping-scam-senate-hearing-jennifer-destefano.

[11] Wikipedia contributors. *Mosaic effect*. Accessed: 2026-01-23. 2025. URL: https://en.wikipedia.org/wiki/Mosaic_effect.

[12] Sohith Vishnu Sai Yachamaneni. *How AI Transforms Fragmented Public Data into Targeted Cyber Threats*. https://drive.google.com/file/d/14LSZ5a6ND23ABGeA7Y-_u_N2QmIe6UfL/view. University of Zurich. Accessed: 2026-01-23. Dec. 2025.