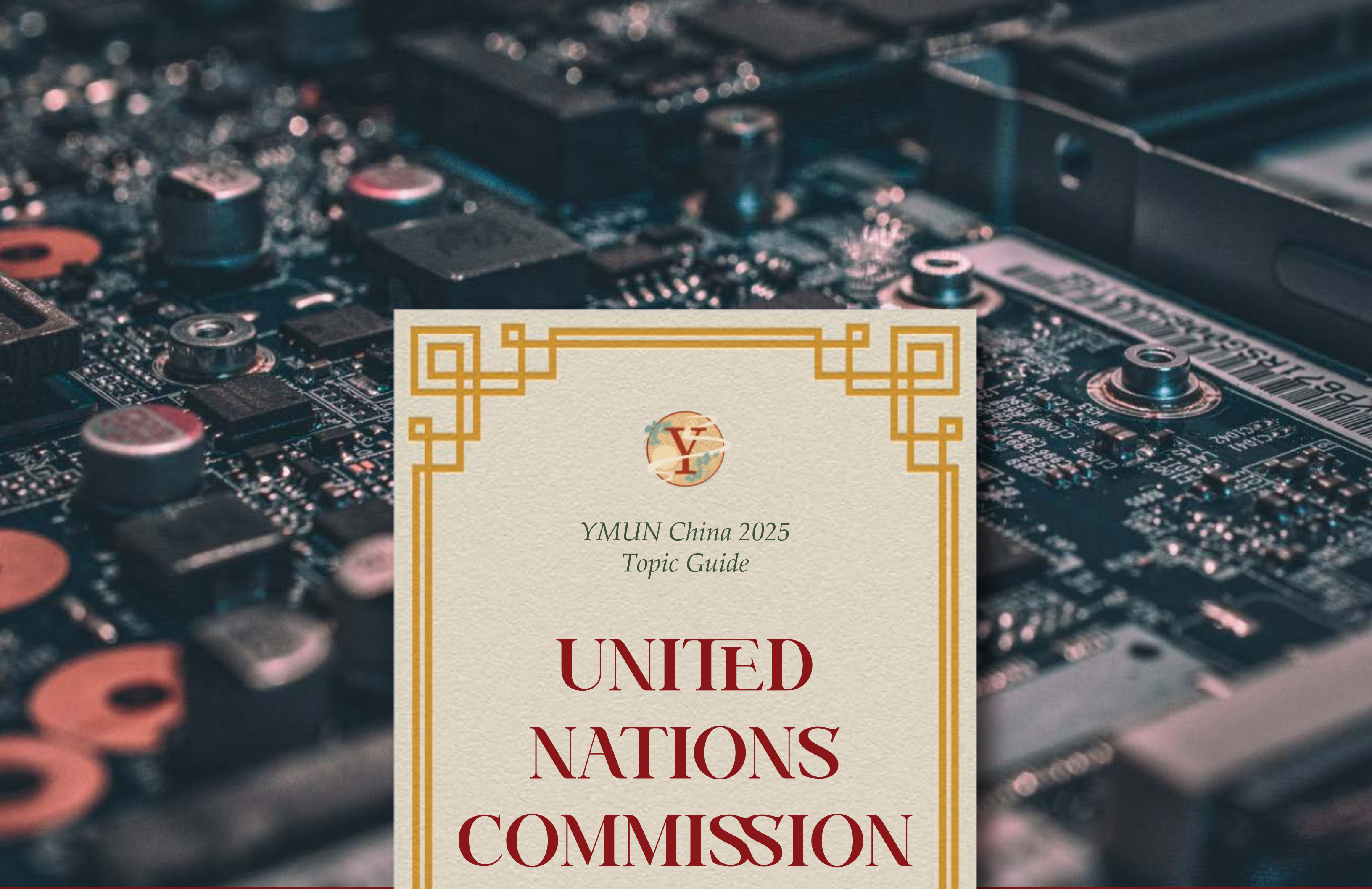


YMUN China 2025
Topic Guide

UNITED NATIONS COMMISSION ON SCIENCE AND TECHNOLOGY

Rifat Tarafder

TABLE OF CONTENTS

Introduction

Topic 1

Topic 2

Letter from the Dais

Dear delegates,

Welcome to YMUN China 2025! My name is Rifat Tarafder and I have the great privilege to serve as the Chair of the United Nations Commission on Science and Technology for Development (CSTD). The CSTD seeks to leverage technological breakthroughs to facilitate sustainable development globally. The goal is simple: to ensure no country is left behind in the age of rapid technological development.

Today, CSTD is focused on the governance of emerging technologies such as AI, big data, and biotechnology, and ensuring their fair and ethical use. The commission is working to address the widening digital divide which has prevented developing nations from harnessing innovation for their development. For example, limited access to AI-powered early disease detection systems and mRNA vaccine production technologies has hindered progress in healthcare. Finally, the CSTD works to foster international cooperation to ensure that science and innovation benefits everyone.

Now, you might be wondering, who is the chair of this super cool committee? My name is Rifat and I am a sophomore from Windsor, Connecticut studying Computer Science, Global Affairs, and Arabic. I am involved with the Yale Computer Society as a lead software developer, the Yale Small Claims Association where we provide legal information to local New Haven residents to help them settle various disputes, and the Yale Muslim Students Association. In my free time, I enjoy watching basketball (my favorite team is the Warriors), going on long drives, and checking out local food spots around New Haven. The reason why I joined YMUN China is to create a memorable conference experience and bring my experience in technology and international relations. I look forward to the thoughtful discussions in our session and I am here to make sure you leave the conference as a more confident leader and informed global citizen.

I look forward to meeting all of you and hope you are as excited as I am for YMUN China. If you have any questions, feel free to contact me at rifat.tarafder@yale.edu with any questions about the conference, committee, Yale, or just to say hello!

Best regards,
Rifat Tarafder

Committee History

The United Nations Commission on Science and Technology for Development (CSTD) is a subsidiary body of the Economic and Social Council (ECOSOC), one of the six main governing bodies of the United Nations. The CSTD holds an annual forum to discuss and debate prominent issues regarding the development and use of groundbreaking technologies.

The UN established the Intergovernmental Committee on Science and Technology for Development in 1979, laying the groundwork for incorporating science and technology in international policy-making. Under Resolution 46/235 in July 1992, the General Assembly consolidated the former Intergovernmental Committee on Science and Technology for Development and its subsidiary advisory committee into the CSTD, making it a functional commission of the ECOSOC.

This structural change demonstrated the UN's commitment to leveraging science and technology to shape a new international economic order and acknowledging its role in fostering international scientific and technological development. Today, the CTSD provides the General Assembly and ECOSOC with consultation, analysis, and policy recommendations on relevant issues. One of the commission’s roles is following up on the outcomes of the World Summit on the Information Society (WSIS). In this role, the CSTD assesses progress made in implementing these outcomes and drafts resolutions for ECOSOC. Another role of the CSTD is analyzing the impact of emerging technologies like artificial intelligence, big data analysis, and the Internet of Things (IoT) on achieving the UN’s 17 goals for sustainable development.

TOPIC ONE

Measures to Combat Cyber Crime

Introduction

In an increasingly digitized world, cybercrime has become a threat to international security, economies, and human rights. Delegates must develop solutions to combat cyber attacks, mitigate the effects of attacks, hold responsible actors accountable, and foster international cooperation.

Glossary

Cybercrime - The use of a computer to perform illegal activities–such as fraud, identity theft, and human trafficking–and new types of crime unique to the cyberspace such as hacking, ransomware, and phishing.

Cybersecurity - Protection of computer software, systems, and networks from threats that can lead to unauthorized data disclosure, theft, damage, or modification.

Malware - Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Ransomware - A type of malware designed to deny access to a computer system until a payment is made; this payment is usually made using a cryptocurrency like Bitcoin or Ethereum.

Backdoor - A covert method of bypassing authentication or encryption in a computer system.

Encryption - The process of protecting data by using mathematical models to obfuscate data such that only the parties who should have access to the data have a way of accessing it.

E2E encryption - A method of encrypting data such that only the sender and receiver have a way of decrypting the data. The data cannot be accessed by any third-party, even the provider of the service.
Cryptocurrency - A digital currency that uses encryption and blockchain technology to enable electronic purchases.
Blockchain - Blockchain is a digital record book shared across a network of computers. It stores information in units called blocks which are connected like a chain. When information is added to the chain, it cannot be modified unless all the computers in the network come to a consensus.

Topic History

Cybercrime has developed rapidly over the past few decades, shifting from isolated occurrences to having global ramifications. One of the earliest instances of technology providing a strategic advantage was during World War II when Alan Turing and Gordon Welchman developed the Bombe (a code-breaking machine) to break the German Enigma code. Historians estimate that their work shortened the war by more than two years, saving over 14 million lives. In 1981, Ian Murphy became the first person to ever be convicted for committing a cybercrime after successfully hacking into AT&T's systems and manipulating the internal clock responsible for managing billing rates. This granted daytime callers late-night discounts while those expecting lower nighttime rates received higher bills.

The first time a computer program was ever weaponized was in 2010 with the creation of the Stuxnet worm. This program was allegedly created by the United States and Israel to disrupt Iranian uranium enrichment facilities. Stuxnet targeted supervisory control and data acquisition systems in these enrichment facilities, gradually sabotaging uranium centrifuges while displaying false information to make everything appear normal. In the past decade, one of the most common types of cyber attack has been ransomware–a type of attack that prevents users from accessing their device and the data stored in it through encryption. Typically, the only way to regain access is by paying the attackers in cryptocurrency.

The most infamous ransomware attacks include CryptoLocker, the first ransomware to be spread through social engineering; SamSam, an attack that destabilized operations in the City of Atlanta and the Colorado Department of Transportation; and WannaCry, the most widespread ransomware attack which affected 200,000 Windows machines in 150 countries, including the UK National Health Service Hospitals.

Current Situation

Cybersecurity and combating cyberattacks has become a major area of focus for the international community, particularly in the past few decades. It has challenged the conventional balance of power among nations. Today, the nations with the most sophisticated technological infrastructure have a significant strategic advantage as technologies like AI enhance military capabilities and intelligence gathering, among others.

Cybercrime Initiatives in the United States

In the United States, the Department of Justice (DOJ) announced a new strategic approach to combating cybercrime, employing an "all means necessary" approach to disrupt cybercriminals and hold them accountable. In its mission statement, the Department highlights the Computer Crime and Intellectual Property Section (CCIPS) as a leader in its efforts in combating cybercrime. The CCIPS has the primary responsibility of curating the Department's cyber and intellectual property offense enforcement strategy, coordinating cyber-enabled crime investigations, and providing legal expertise through case summaries, legislative analysis, and creating digital training programs for other prosecutors within the Department. The Money Laundering and Asset Recovery Section (MLARS) aids the Department in combating cybercrime with its expertise in emerging technologies such as blockchain and cryptocurrency, as well as the tracing, seizure, and forfeiture of assets. Finally, the Department fosters international cooperation in addressing cybercrime through the Office of International Affairs (OIA) which is responsible for coordinating with foreign partners, collecting foreign evidence, and ensuring the arrest and extradition of actors that may flee overseas.

International Cybercrime Initiatives

Members of the international community are also strengthening their cybersecurity measures. In December 2024, the United Nations General Assembly adopted resolution 79/243 which established the Convention against Cybercrime. This is one of the first UN treaties of its kind, providing Member States with a comprehensive range of measures to prevent and combat cybercrime and strengthening international cooperation, especially in sharing digital evidence in severe crimes. The signing ceremony for this treaty will likely be held mid-2025 in Vietnam. States will then ratify the treaty and it will enter into force once 40 States become Parties.

The Budapest Convention on Cybercrime is the first international treaty addressing internet crimes, consolidating the national laws of various nations, and increasing cooperation among states. The treaty was drafted in France by the Council of Europe with active involvement from observer nations including Canada, Japan, and the United States. The Convention was adopted in November 2001 and entered into force, with ratification from 78 states. Although the mission of the Convention is benign, key nations such as India and Russia have declined to adopt the Convention as they did not help draft it, and Russia stating that it is a threat to its sovereignty; this highlights a major challenge in promoting international cooperation as it requires the mindfulness of the interests of several parties, some of whom may have conflicting objectives. The goal of the Convention is to address internet crimes, specifically copyright infringements, computer fraud, hate crimes, propaganda, and computer network security. It also outlines procedures to preserve stored data, traffic data, and content data, search and size of computer data, and real-time collection of traffic data.

Individual nations have begun ramping up cybersecurity efforts. One example is the Australian Federal Police (AFP) which has been proactive in investigating cybercrime, with over 100 active investigations in December 2024. The AFP estimates that its efforts have prevented over $80 million in losses. Another example is the United Kingdom which recently passed the Cyber Security and Resilience Bill in July 2024 with the goal of strengthening existing cybersecurity frameworks while putting an emphasis on the protection of critical infrastructure.

With all of these legislative bodies and initiatives in place, what has the international community done in response to cybercrimes, and how has the international community leveraged technology to address other forms of crime? To answer this question, we will examine various cyber operations that had global ramifications and the subsequent response from the international community.

Case Study: NotPetya Attack (2017)

For almost a decade, Russia and Ukraine had been engaging in a “silent conflict” until it developed into a full-scale war in February 2022. Between 2015 and 2016, a Russian group known as “Sandworm” hacked into Ukrainian governmental agencies and companies with victims ranging from ordinary civilians to large media outlets and corporations. Some of their various tactics included detonating logic bombs that erased terabytes of data and attacking critical infrastructure in the winter, causing widespread power outages. The most notorious malware to emerge from this testbed was NotPetya.

In 2017, Russian military hackers gained access to the servers of a company called Linkos Group. This company specialized in creating accounting software, with its most popular application being M.E.Doc. By gaining access to the Group’s servers, they installed a backdoor into the machines of millions of M.E.Doc users, allowing them to deploy the NotPetya malware. It quickly became one of the fastest-transmitting pieces of malware in history. NotPetya utilized two exploits. The first exploit was called EternalBlue, a cyberweapon developed by the US National Security Agency to gain remote access to a Windows machine through a vulnerability in the operating system. This weapon was highly classified until it got leaked earlier that year by a group known as the “Shadow Brokers”. The second exploit was called Mimikatz. This exploit took advantage of a Windows vulnerability that left users’ passwords in the computer’s memory, allowing hackers to gain access using those credentials. The goal of NotPetya was to encrypt a machine’s master boot record, which contains the necessary information to start a computer. The malware then instructed users to pay a ransom to regain control of the machine, even though there was no way to decrypt and recover it.

Within hours of its release, NotPetya escaped the borders of Ukraine and infected a countless number of machines around the world. Most of the victims were organizations based in the United States and Europe including FedEx, Saint-Gobain (a French construction company), and food producer Mondelez. It is estimated that NotPetya inflicted financial damages amounting to $895 million in Ukraine and another $1 billion worldwide. Following the attack, the NATO Cooperative Cyber Defense issued a statement formally condemning the attack and attributing it to Russian actors. Subsequently, in a speech delivered by NATO Secretary-General Jens Stoltenberg, he encouraged Allies to develop and refine their own cyber capabilities. He also emphasized the possibility of a cyberattack triggering Article 5, the NATO collective defense clause. Although this is a possibility, legal scholars are still attempting to define the context in which a cyberattack can be considered an act of war and applying existing international frameworks to the cyberspace, especially when it comes to state sovereignty and the principle of non-intervention.

The NotPetya attack primarily served as a wake-up call for the international community and brought attention to the need for strengthening cybersecurity initiatives and addressing the future of cyber warfare.

Case Study: Operation Trojan Shield (2021)

In 2018, the FBI spearheaded the largest international sting operation in history, intercepting millions of messages through a secure proprietary communication service mainly used by criminals. In collaboration with law enforcement agencies across the world, the operation led to the arrest of over 800 individuals suspected of criminal activity in 16 countries. How did the FBI accomplish this feat? It started with a Canadian messaging company called Phantom Secure. This company developed special phones with the flagship feature being total encryption of device data, including all communications. Phantom Secure sold exclusively to international criminal organizations because of the high demand for encrypted devices and their deterrence against government surveillance. The company was taken down by the FBI in 2017, leaving a gap in the market for secure communications devices.

Around the same time, the FBI apprehended a hacker by the pseudonym "Afgoo" who was developing a new encrypted device for criminal networks following the shutdown of Phantom Secure. The app on this device was called ANOM, a secure communication service which offered features like E2E encryption, auto-deleting messages, and voice notes that masked the user's real voice. Afgoo decided to cooperate with the FBI in exchange for a reduced sentence, so the FBI built a backdoor into the platform, allowing them to decrypt and store messages being sent in real-time without needing physical access to the device. US law prohibits federal agencies from surveilling foreign nationals, so the FBI worked with the governments of Australia, Lithuania, and a third unnamed European country to develop the backdoor and gain access to the messages.

ANOM devices became popular among criminal networks through word of mouth. It began with undercover agents advertising the device. Hakan Ayik, a notorious Australian drug dealer, was identified as a person of interest in terms of distributing the device. He was encouraged by undercover agents to use the device, and once he believed in the legitimacy of ANOM, he began selling them on the black market. By May 2021, almost 12,000 ANOM devices were in use. By this time, the FBI began collaborating with law enforcement agencies worldwide to analyze the messages, gather evidence, issue search warrants, and coordinate arrests.

On June 8, 2021, the FBI announced the end of Operation Trojan Shield. The operation led to the arrest of 800 individuals in 16 countries; these individuals were suspected of being members of the Italian mafia, Albanian organised crime, drug syndicates, human trafficking groups, among others. The seized evidence included over 40 tons of drugs, firearms, luxury vehicles, and stolen cash. Although the operation was successful, it raised several questions around privacy, the use of malware by law enforcement, information-sharing between foreign governments, and indiscriminate surveillance. The operation, which was targeted at transnational criminal networks, compromised the privacy of unaffiliated citizens who used ANOM devices without knowing of their intended purpose. The information collected was shared between US and Australian authorities, nations with explicit laws prohibiting foreign information-sharing.

Through these case studies, we can gather that the increasing weaponization of cyber tactics in geopolitical conflicts is a matter that must be given attention to. International norms on cyber warfare and state-sponsored attacks must also be a priority. Through this topic, delegates will have the opportunity to craft strategies that foster public-private partnerships, uphold human rights, and ensure equitable access to cybersecurity resources, all while navigating geopolitical tensions over digital sovereignty.

Questions to Consider

1. What is the threshold for a cyber operation to be considered an act of war?
2. What are some legal, political, cyber, and economic responses a state can take to deter other rogue states from pursuing destructive cyber operations in the future?
3. To what extent should governments be allowed to use backdoors and malware to combat cybercrime? How can we balance security and privacy?
4. How should cyber insurance policies be structured? What are the challenges in determining liability and coverage for state-sponsored attacks?
5. Given the nature of cyber attacks, should international security alliances include them in collective defense agreements?
6. How can nations develop counter-cyber warfare initiatives that maximize global cooperation?
7. What are the ethical and legal implications of governments developing and deploying cyberweapons?

Additional Resources

https://lawreview.law.ucdavis.edu/archives/57/3/law-trojan-horse#:~:text=While%20the%20scope%20of%20police,when%20it%20cannot%20be%20used.

https://www.ibm.com/think/topics/blockchain

https://www.sciencedirect.com/topics/computer-science/cryptocurrency#:~:text=In%20subject%20area%3A%20Computer%20Science,the%20history%20of%20transactions%20securely.

https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance/

https://www.monroeu.edu/news/cybersecurity-history-hacking-data-breaches

https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/

https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive

https://www.unodc.org/unodc/en/cybercrime/convention/home.html

2

TOPIC TWO

Digital Innovation in Education

Introduction

With the rise of the internet and online learning platforms, education has become more accessible and inclusive than at any other point in history. However, disparities in internet access and digital literacy prevents millions from taking advantage of these advancements, widening the digital divide.

Glossary

Digital divide - The digital divide is the gap between people who have access to affordable, reliable internet service (and the skills and devices necessary to take advantage of that access) and those who lack it.

Personalized learning - Customizing the learning experience for each student based on their unique skills, abilities, and preferences.

Computer-Assisted Instruction (CAI) - Any form of instruction that is presented on a computer; it usually involves online tutorials that allows users to engage in self-directed learning.

Machine learning - A branch of artificial intelligence focused on allowing computers to imitate the way humans learn new things. The goal of machine learning is to allow computers to make the best decision based on the data it has been trained on.

Large language model - Artificial intelligence systems capable of understanding and generating human language by processing large amounts of text data.

Open Educational Resources (OER) - Openly licensed educational materials that anyone can use, modify, and distribute.

Algorithmic bias - Unintended bias in AI-powered educational tools that can result in unfair evaluations and unequal learning opportunities.

Digital literacy - The ability to effectively use digital tools. This includes understanding the basics of AI, cybersecurity, and online research skills.

Topic History

Although the concept of digital education has been popularized in the past two decades, the desire to improve accessibility to education has been around for centuries. Distance learning has been around long before the internet. The earliest recorded instance of a distance learning program was in 1728 when Caleb Phillips taught a series of courses for shorthand writing. These courses consisted of weekly lessons sent by mail and were advertised in the Boston Gazette. By this time, distance learning had become very popular, allowing people from around the world to develop new skills regardless of their location. In 1858, the University of London began offering degree courses through their External Programme allowing anyone outside of London to earn a degree from the university. The term "distance learning" was first coined by the University of Wisconsin in 1892. Wisconsin was among the first universities to use phonographs, a relatively new technology at the time, to record and distribute lectures to students. Although distance learning was becoming popular, it was still only limited to individuals who had both the literacy and financial means to afford course materials, postal services, and the time to complete these courses.

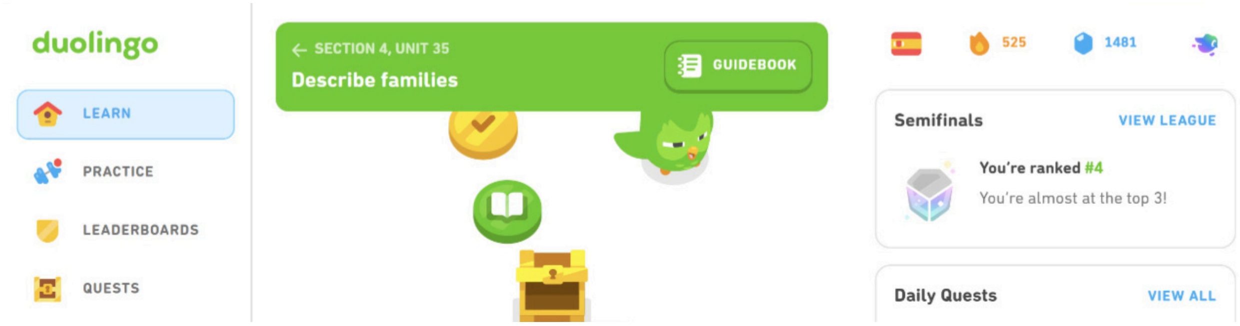
The first true innovation in digital education came with the advent of Computer-Assisted Instruction (CAI). The idea of CAI was to create computer programs that prompted a student with a question, the student inputs their response, and the program outputs whether the answer was right or wrong. The program would keep track of a student's progress and provide questions that would align with the student's knowledge and skill level. The IBM 1500 instructional system was introduced in March 1966 and was IBM's attempt to implement CAI. The system was initially prototyped in an elementary school before it was shipped to Stanford University a year later in August 1967. The main appeal of the IBM 1500 was that it allowed teachers to remotely send course materials, evaluate assignments, and organize documents. The 1980s saw the greatest innovations in digital education when the University of Toronto offered the first fully online course. Following this, the University of Phoenix became the first educational institution to establish online bachelor's and master's degree programs in 1989, making higher education much more accessible to the public.

Current Situation

The field of education technology and demand for innovative learning solutions has grown exponentially in the past few decades. This growth has been facilitated by the internet, which has empowered millions to learn new skills, whether it be for a new hobby or to explore a new career path. Today, anyone with an internet connection can access computer science courses taught at MIT through platforms like edX, or learn a language they would have never been able to otherwise through Duolingo.

Current Digital Education Landscape

With the rise of the World Wide Web in the 1990s to early 2000s, educational institutions saw this as an opportunity to curate and deliver online courses. Platforms like Blackboard and Moodle were the first of their kind–learning management systems that transformed the way instructors create, distribute, and manage course materials, assignments, and student engagement. Around this time, universities began offering online degree programs, allowing students to pursue higher education without the need for in-person attendance. These developments set the stage for the acceleration of online learning starting in the early 2000s. One of the most well-known online learning platforms is Khan Academy. What started as a side project of recording YouTube videos to tutor his cousins remotely, Sal Khan transformed into Khan Academy, a nonprofit backed by Google and the Bill and Melinda Gates Foundation dedicated to providing a free, world-class education to everyone. Khan Academy covers a variety of subjects ranging from history and art to engineering and the natural sciences. What separates Khan Academy from other platforms is the breadth of its content translated into 20+ languages, as well as its points and badges system, step-by-step problem guides, and instant feedback on assignments.



You're ranked #4

You're almost at the top 3!

Duolingo is another platform that has recently revolutionized how people learn languages. Created in 2011 by Luis von Ahn and Severin Hacker, Duolingo quickly gained popularity and has become the world's most downloaded education app. By essentially turning language-learning into a game through incentives like daily streaks and a widely-recognizable mascot, Duolingo has made this activity accessible and enjoyable for people of all ages and language backgrounds; this gamification has only helped Duolingo's user retention rate and keeps students motivated and willing to come back the next day for another lesson. Although Duolingo boasts over 500 million users, it still has room to grow–over 2 billion people are studying a foreign language and many of them are doing it online. The digital language-learning industry generates around $6 billion and this figure is projected to grow to $8.7 billion by 2025.

Entrepreneurs are not the only ones making innovations in the field of education technology. The OpenCourseWare (OCW) movement began in 1999 when the University of Tübingen published videos of lectures to their Tübinger Internet Multimedia Server. The movement gained traction in 2002 when MIT launched its own iteration of OpenCourseWare with the goal of enhancing education worldwide by "the availability of a web of knowledge"; other big-name institutions followed suit include Yale University, the University of Michigan, and the University of California, Berkeley, among others. Capitalizing on the success of OpenCourseWare, Anant Agarwal, a professor at MIT, developed a similar platform called edX. MIT OCW and edX differ in certain aspects including format and structure, certifications, and interactivity. edX offers structured online courses with video lectures taught by professors, as well as quizzes, assignments, and discussion forums while OCW only offers self-paced access to course materials from MIT classes. edX also offers certificates and paid online degree programs. The most popular edX course of all time is Harvard's CS50 Introduction to Computer Science which has reached over 5 million people across the world through edX, OCW, and YouTube.

Education during COVID-19

The COVID-19 pandemic only exacerbated the demand for online education infrastructure as schools and universities around the world were forced to pivot to remote instruction. This sudden shift increased the demand for services like Zoom and Google Classroom, and made online learning a ubiquitous part of the educational landscape. The latest, and arguably most profound, development in digital education is ChatGPT, and more generally, large language models (LLMs) like Google Gemini, Claude, Microsoft Copilot, and Deepseek, among dozens of others, each with its own speciality (writing, coding, research, data analysis, etc).

Large language models are an area of focus within education because of their diverse range of applications. These models have the ability to enhance learning and teaching experiences for people across all levels of education, as well as learning preferences, abilities, and needs. At the primary school level, large language models can aid in reading and writing skills by suggesting syntax and grammar corrections, generate reading response questions that engage critical thinking skills, and provide summaries of complex texts to improve comprehension. At the secondary school level, large language models can help with a variety of subjects like mathematics, biology, chemistry, language, and literature by generating practice problems, explanations, and step-by-step solutions. At the university level, these models can help with research, brainstorming ideas for papers, and generating supplemental summaries for readings. LLMs can also be used to empower learners with disabilities; for example, speech-to-text and/or text-to-speech solutions can help people with visual impairment. Given the accessibility of LLMs, anyone can tweak and customize them to become their own personal tutor. Coupled with immersive technologies like augmented reality (AR) and virtual reality (VR), the future of digital education appears to be heading in a direction that emphasizes intractability, personalization, and accessibility.

Ethical Concerns in Digital Education

Although these up-and-coming AI education solutions are exciting and carry endless possibilities, it is also important to consider the ethical concerns associated with these innovations. One concern is data privacy and security. Zoom has faced public backlash on several occasions over the last five years for its handling of user data. Among the many features of Zoom, one of its newer features uses machine learning to generate live subtitles, transcripts, and meeting summaries. Many were concerned that their meetings would be used to train Zoom's machine learning models. Although Zoom stated it would never use customers' data without their consent to train their models, customers cited the company's updated terms of service which stated that users agree to "grant Zoom a perpetual, worldwide, non-exclusive, royalty-free, sublicensable, and transferable license" for various purposes, including "machine learning, artificial intelligence, training, testing, improvement of the Services, Software, or Zoom's other products, services, and software." This criticism is a part of a larger uncertainty of how people's data could be used to train LLMs without their consent or any form of compensation.

The rise of AI has also raised concerns of whether it will support educators or replace them. Proponents of digital education argue that technology is a powerful aid to educators because AI-powered platforms can create personalized learning experiences for students, automate administrative tasks like grading and assignment feedback. Critics argue that over-relying on technology reduces teacher-student interaction and emotional support, and increases the gap in educational inequality. More well-resourced schools can invest in educational models that adequately blend technology and human interaction in a way that supports teachers. Underfunded schools may be inclined to cut costs by using AI platforms instead of bearing the cost of hiring and training teachers, reducing human interaction in the classroom. Another concern is algorithmic bias in AI grading systems. On the surface, AI-assisted grading is an efficient solution for teachers as it provides instant grading and assignment feedback, circumventing hours of manual grading.

However, AI bias could hurt students who have different writing styles or come from different cultural backgrounds. There are also concerns about data privacy and collection of student work by institutions. A dangerous side effect of an over-reliance on AI is students tailoring their work to please the algorithm rather than develop an understanding or appreciation for the material.

The Digital Divide

The digital divide is the gap between people who have access to affordable, reliable internet service (and the skills and devices necessary to take advantage of that access) and those who lack it. This gap exists for a number of reasons such as geographic location, existing differences in wealth, access to education, and discrimination based on gender and race. The global digital divide can be attributed to economic development. Incomes have risen across the world in the past 20 years, and the expectation was that as countries and individuals became richer, they would purchase digital capital and invest in technological infrastructure, bridging the gap naturally.

Unfortunately, internet penetration rate still varies drastically by continent. In 2024, 91% of Europeans have internet access compared to 38% of Africans. Even these statistics vary by region as countries by the coast have better internet access compared to landlocked countries. The digital divide comes with several consequences. In a world where millions connect with each other through social media, the COVID-19 pandemic showed that those without internet access face digital isolation. As education rapidly digitizes, those without the resources to access the internet, including students studying remotely during the pandemic, could be cut off from opportunities to develop their skills. This can exacerbate educational gaps among students and limit job opportunities for adults.

Global Policy Initiatives

In recent years, there have been efforts to bridge the digital divide. The UN Sustainable Development Goal 4 aims to “ensure inclusive and equitable quality education and promote lifelong learning opportunities for all.” To fulfill this mission, UNESCO leads multiple initiatives including the Global Education Coalition, the Open Educational Resources (OER) initiative, and AI in Education Guidelines.

The Global Education Coalition was established in March 2020 to respond to disruptions in education caused by the COVID-19 pandemic. The Coalition consists of a network of 220+ institutions across the UN, academia, and private sector. It is active in 112 countries and has helped 800,000+ youth with professional development, trained 790,000+ teachers, and provided STEM learning resources to 1,000,000+ students. The AI in Education Guidelines lays out ethical frameworks for the use of AI in education that address equity, data privacy, and avoiding bias in automated grading systems.
Governments around the world are implementing national policies to bring digital tools into their existing school curriculums.

In the United States, the Federal Communications Commission (FCC) funds programs that provide schools with affordable and reliable internet access. Additionally, the 2021 Digital Equity Act and 2021 US Infrastructure Investment and Jobs Act allocates billions in funding to ensure low-income and rural communities have adequate broadband access. In the European Union, schools are experimenting with hybrid learning models and leveraging AI to support teachers.

The European Union also has the strongest data protection regulations in the world with its General Data Protection Regulation (GDPR); it is actively promoting cybersecurity and data protection in digital education to address concerns over student privacy.

In China, companies like Tencent and Alibaba are creating the future of AI-powered education through their digital tutoring platforms. The Chinese government is also rolling out their own nationwide online learning platforms. Private companies are also partnering with governments in developing and distributing digital education solutions. Some of these initiatives include Google for Education which works with governments to provide schools with Google Classroom and Chromebooks, Microsoft's AI for Education, and Starlink which works with governments to provide satellite internet to some of the most remote regions on the planet.

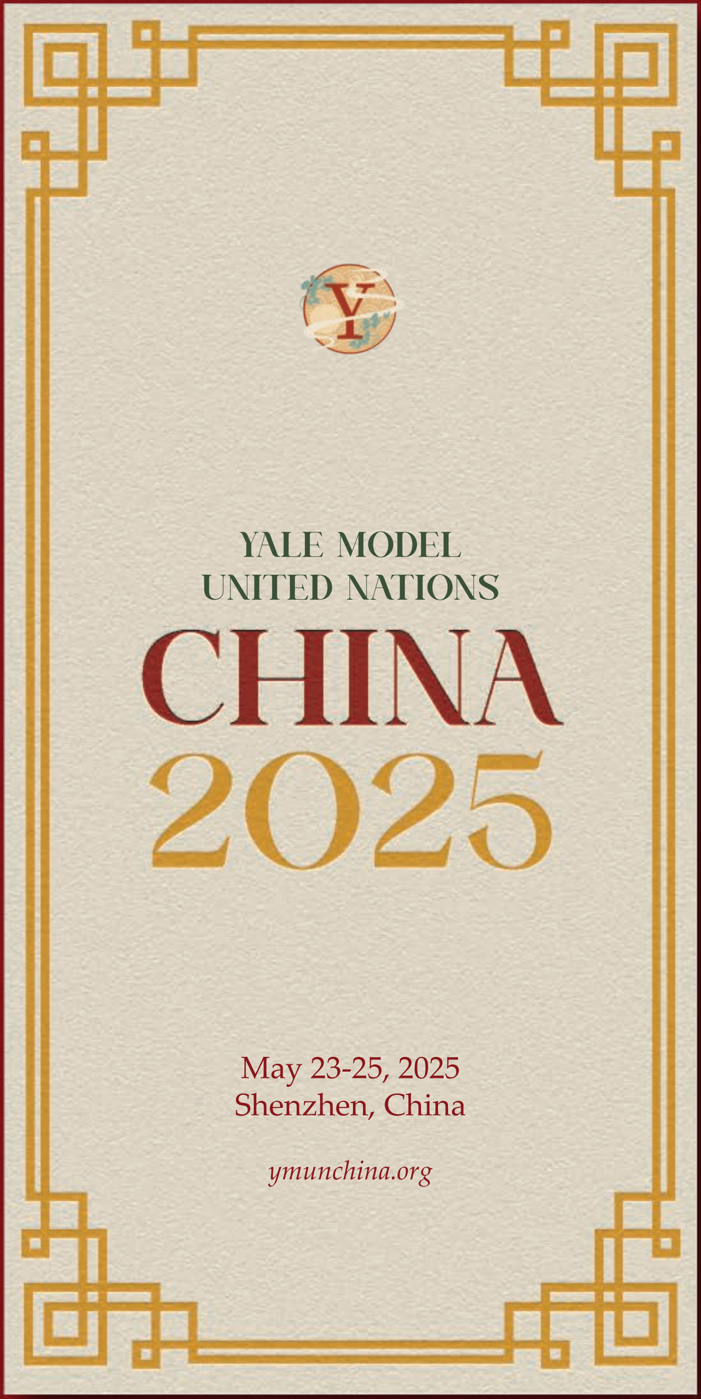
Through this topic, delegates will face the unique challenges that come with balancing rapid innovation with inclusivity, ensuring digital tools advance Sustainable Development Goal 4 (quality education) without leaving vulnerable populations behind. Creativity and collaboration will be key to reimagining education in the 21st century.

Questions to Consider

1. Many governments are investing in digital infrastructure in order to bridge the digital divide. Should internet access be considered a fundamental human right in the 21st century? Who should bear the cost of installing this new infrastructure: governments, private companies, or international organizations?
2. How can governments regulate the extent to which AI replaces teachers? What is the line between enhancing teachers and replacing them?
3. Technology companies like Google and Microsoft have a significant role in digital education by offering services like cloud storage and communication platforms. Should governments limit this corporate influence in public education? How can we ensure that the public interest is preserved?
4. Many innovations in digital education are pioneered in Western nations. How can we ensure these tools are culturally inclusive and diverse in order to avoid this notion of “educational colonialism”?
5. What legal safeguards can be put into place to prevent the misuse of student data by private technology companies and governments?
6. Should wealthier countries and private technology companies be required to subsidize digital education in developing countries?
7. Should digital literacy be a required subject in the 21st century?

Additional Resources

https://www.researchgate.net/publication/382017625_Ethical_Considerations_in_Digital_Education
https://bera-journals.onlinelibrary.wiley.com/doi/10.1111/bjet.13370
https://ctu.ieee.org/blog/2022/12/14/what-is-the-digital-divide/
https://www.weforum.org/stories/2024/07/artificial-intelligence-education-teachers-union/
https://www.researchgate.net/profile/Saddam-Issa-2/publication/380320150_Digital_initiative_literacy_and_gender_equality_Empowering_education_and_language_for_sustainable_development/links/66354ac706ea3d0b74256352/Digital-initiative-literacy-and-gender-equality-Empowering-education-and-language-for-sustainable-development.pdf
https://essuir.sumdu.edu.ua/bitstream-download/123456789/93171/1/Melnyk_SEC_3_2023_1.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2814822



YALE MODEL
UNITED NATIONS

CHINA 2025

May 23-25, 2025
Shenzhen, China

ymunchina.org