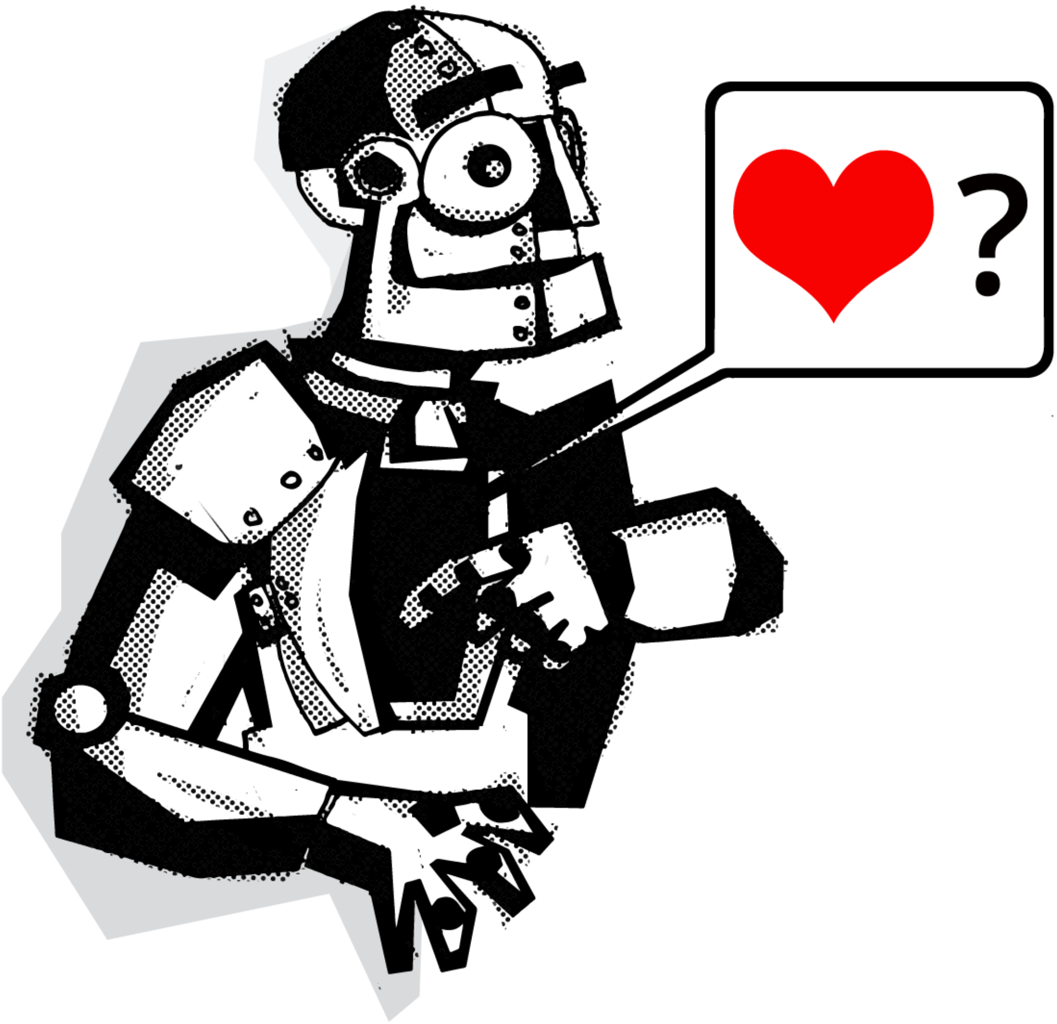
GENEVA INTERNET PLATFORM
digwatch

NEWSLETTER

Issue 71, **July 2022**



Has AI become sentient?

Pages 6–7

TRENDING

Africa as a centre of digital policy, AI and its (alleged?) sentiency, and content policy were the trending topics in June.

Pages 2-3

IN FOCUS

How fast do we need the same customer protection for crypto finance as traditional finance?

Pages 8-9

REFLECTIONS

Europe's regional internet governance initiative met in situ after three years. The GIP brings you a report from the ground

Page 10

GENEVA

Many policy discussions take place in Geneva every month. We bring you a roundup of the latest news from International Geneva.

Page 11

Top digital policy trends

1. Africa as one of the centres of digital policy

There is a paucity of African voices in global digital policy processes – participation has been lacking, particularly meaningful participation in discussions on issues such as standardisation, cybersecurity, and artificial intelligence (AI). However, this is changing. More countries are participating in the UN Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security. The Internet Governance Forum (IGF) will be held in Addis Ababa in November 2022. There is a vibrant technical community in Africa, which represents the interests of their countries. There are many building blocks; the challenge for Africa is how to put these building blocks together using an inclusive, broader, multilateral, multistakeholder approach by maximising talents. This could also be identified as a challenge for many other countries, because participating in digital negotiations is becoming extremely demanding in terms of resources, policy experience, and institutional capacities.

A major challenge for African leaders and stakeholders is framing the discussion around their development needs. Past debates have focused on infrastructure development in the continent. There will be more and more fibre optics and broadband coming to the landlocked and remote regions of Africa, but in the coming year, the discussion will likely shift from simply making connections to ensuring that the interests of people who are connected to the internet are protected, and that they are encouraged to use digital networks meaningfully for education, health, business, etc.

The portfolio of topics that are of interest in Africa is broadening to cybercrime, usability, education, e-commerce, and digital identities. These discussions are becoming increasingly sophisticated. Africa is the continent for future digital growth in terms of new internet users, new businesses, and new applications. It is the responsibility of the global community and the UN to showcase these examples and to give them more prominence in the media. More discussions about Africa as a new space to create inclusive impactful digital developments are needed, instead of discussions about Africa as a geopolitical space or a fight between two major digital powers – China and the USA – as it is traditionally framed.

2. AI and sentiency

Google engineer Blake Lemoine caused a right fuss when he claimed that Language Models for Dialog Applications, or LaMDA – a system Google is developing to generate chatbots – has become sentient and has a mind of its own. Do we need to fear machines taking over the world? Or should we be more concerned about the misuse of AI and deepfakes? For example, the last week of June saw mayors of large European cities duped into a conversation with a deepfake of Kyiv mayor Vitali Klitschko. The FBI has issued a warning that cybercriminals are using deepfakes to apply for remote tech jobs to gain access to confidential information.

Diplo’s AI and Data Lab explains more about LaMDA and weighs in on the sentiency debate on pages 6 and 7.

3. Digital in high politics

Content policy garnered much attention in June as well, with new rules and codes coming from China, India, Nigeria, and the EU.

China updated the regulations for mobile apps. App providers and distributors must promote fundamental socialist ideals and follow 'proper' politics. App creators are responsible for the content on the app, and they shouldn't create or distribute illegal information. The rules will be effective starting 1 August 2022.

China also introduced new rules for influencers and the live-streaming industry. Influencers will need to have relevant qualifications to be able to discuss topics such as medicine, law, finance, and education. Certain types of online behaviour will be completely banned, such as publishing content that weakens or distorts the leadership of the Chinese Communist Party, the socialist system, or the country’s reforms; using deepfake technology to tamper with the images of party or state leaders; or showing extravagant lifestyles. Livestreamers are also required to declare their incomes and comply with tax obligations. Moreover, online platforms should refrain from ‘giving public figures who have violated the law or shown “no ethics”, the opportunity to express their opinions publicly, hold performances, create a new account or switch to another platform’.

India proposed [new rules for internet intermediaries](), setting forth new obligations for intermediaries and a redress mechanism for users:

- Intermediaries are required to ensure that users comply with the intermediary’s rules and regulations, privacy policy, and user agreement.
- Intermediaries are required to protect the rights guaranteed to users under India’s constitution.
- Intermediaries are required to acknowledge user complaints within 24 hours through grievance officers, address a complaint for the removal of content within 72 hours of the receipt of the user’s complaint, and implement safeguards to prevent user misuse of the grievance redressal mechanism.
- If a user disagrees with the grievance officer's decision, they have 30 days to file a complaint with the government's new grievance appeals mechanism, the Grievance Appellate Committee.
- Users will still be able to take their complaints directly to a court of law if they disagree with the intermediary's decision.

Nigeria’s National Information Technology Development Agency (NITDA) released a draft code of practice for online platforms. The code aims to protect the ‘fundamental human rights of Nigerians and non-Nigerians living in the country’ as well as ‘safeguard the security and welfare of Nigerians while interacting on these Platforms.’ The code also outlines the conditions online platforms must fulfil to operate in Nigeria:

- Establish a legal entity; in other words, register with the country’s Corporate Affairs Commission (CAC).
- Appoint a designated country representative to interface with Nigerian authorities.
- Abide by all regulatory demands after establishing a legal presence.
- Comply with all applicable tax obligations on its operations under Nigerian law.
- Provide a comprehensive compliance mechanism to avoid publication of prohibited content[s] and unethical behaviour on their platform.
- Provide information to authorities on harmful accounts, suspected botnets, troll groups, and other coordinated disinformation networks and delete any information that violates Nigerian law within an agreed time.

Twitter, Facebook, WhatsApp, Instagram, Google, and TikTok were asked for input during the drafting of the code. For more details about the genesis of the code, watch our latest IG briefing with Emmanuel Edet, Assistant Director at NITDA.

The European Commission updated its Code of Practice on Disinformation, with its 34 signatories, such as Facebook, Twitter, Google, Microsoft, and TikTok, jointly revising the voluntary code of practice from 2018. Signatories must commit to a list of obligations such as demonetising advertisements containing disinformation, making more data accessible to researchers, empowering users and fact-checkers to spot and flag non-factual information, and making public their implementation efforts via a transparency centre. The code also encourages cross-service cooperation among the signatories to reduce manipulative behaviours, such as malicious deepfakes, bot-driven amplification, and impersonation. The European Commission has stressed the voluntary nature of this code; it welcomes, yet does not endorse the result. A task force, chaired by the Commission and composed of representatives of the signatories and specialised EU agencies, will follow up with regular assessments of progress regarding the code. The Digital Services Act (DSA) will enforce the code.

Content policy has been among the top three digital trends since January, and it is not likely to lose relevance anytime soon. For example, a new situation tech companies have found themselves in with the US Supreme Court overturning Roe vs Wade (meaning that the constitutional right to abortion does not exist in the USA) is what to do about abortion-related posts from users. For now, we have seen Facebook and Instagram remove posts offering abortion pills.

Barometer

Digital policy developments that made headlines

The digital policy landscape changes daily, so here are all the main developments from June. We've decoded them into bite-sized authoritative updates. There's more detail in each update on the Digital Watch observatory.

Increasing relevance

Global digital governance architecture

Cybersecurity, the digital economy, and advanced technologies featured on the agenda of the BRICS 2022 Summit. At the G7 Summit, leaders discussed digitalisation.

The UN Secretary-General appointed Amandeep Singh Gill as his Envoy on Technology.

Low relevance

Sustainable development

The World Telecommunication Development Conference concluded with the adoption of the Kigali Action Plan and several resolutions to advance connectivity and digital transformation.

Increasing relevance

Security

Cloudflare detected and mitigated the biggest distributed denial of service (DDoS) cyberattack over HTTPS on record.

The head of the US Cyber Command confirmed that the USA has conducted cyber operations in support of Ukraine. Russian hackers allegedly launched attacks against targets in Lithuania and Norway.

NATO countries established a 'virtual rapid response cyber capability to respond to significant malicious cyber activities', on a voluntary basis and using national assets.

The International Red Cross and Red Crescent Movement called on state and non-state actors to refrain from cyber operations against humanitarian organisations.

Increasing relevance

E-commerce and the internet economy

Japan passed a law clarifying the legal status of stablecoins. The UK published a proposal to adapt existing rules to be able to deal with stablecoin collapses. Singapore launched a digital assets initiative.

The Swiss Federal Supreme Court upheld a ruling according to which Uber should be regarded as an employer.

China adopted a plan to promote the regulation and 'healthy development' of fintech.

Barometer

Infrastructure

Low relevance

Plans are underway for a submarine cable connecting Egypt and Saudi Arabia.

EU institutions reached a political agreement on the introduction of a requirement for a common charger for digital devices.

Digital rights

Increasing relevance

The Office of the UN High Commissioner for Human Rights urged countries not to impose internet shutdowns.

The Italian data protection agency (DPA) found that using Google Analytics means unlawfully transferring data to the USA. In Russia, Google was fined for breaching data localisation rules.

Argentina's Supreme Court ruled that the right to be forgotten can infringe on freedom of information.

Content policy

Increased relevance

The US Supreme Court blocked the controversial Texas social media law.

The EU regulation on addressing the dissemination of terrorist content online entered into force.

Wikipedia appealed against a Moscow court decision demanding it remove content related to the Ukraine war. Meta lost an appeal in a Moscow court after being found guilty of 'extremist activity'.

Jurisdiction and legal issues

Low relevance

The EU General Court cancelled the €1 billion fine the European Commission imposed on semiconductor company Qualcomm in 2018.

The UK launched an anti-competition investigation into Google's distribution of apps on Android devices. Germany launched a proceeding against Apple to examine the company's App Tracking Transparency Framework.

New technologies

Increased relevance

Microsoft updated its Responsible AI Standard and limited access to facial recognition tools. Spain launched an AI regulatory sandbox.

Singapore launched two new quantum computing initiatives. The UK acquired its first quantum computer. Germany will host Europe's first exascale computer.

A Metaverse Standards Forum was launched to foster the development of open standards for the metaverse.

Russia limited exports of chip-relevant noble gases, while Taiwan strengthened ties with the EU and the USA.

In focus

Has AI become sentient?

The huge hype about AI exists for a reason. In recent times, there has been significant progress in many areas, in particular computer vision – more precisely self-driving cars, robotics, and natural language processing (NLP).

In the field of self-driving cars, there are five levels of driving automation. If a vehicle has Level 0, Level 1, or Level 2, an active and engaged driver is still required, so the vehicle does not make decisions in every situation on its own. We are currently at Level 2, which applies to vehicles with advanced driving assistance systems (ADAS) that can take over steering, acceleration, and braking in specific scenarios, but the driver must supervise those actions. The driver needs to perform tactical manoeuvres, such as responding to traffic signals, changing lanes, and scanning for hazards. In the future, the unsupervised system would have Level 3, Level 4, or Level 5, which corresponds to automated driving systems where the technology takes complete control of the vehicle without human supervision. This is, of course, a huge improvement, but it is far from full automation.

NLP is one of the most exciting fields in AI and has already given rise to technologies like chatbots, voice assistants, translators, and many other tools we use every day. When we talk about breakthroughs in this field, we must mention Attention is all you need – a research paper published by Google AI employees in June 2017. It was the first time the concept of transformers was referenced. In NLP, the transformer is an architecture that aims to solve sequence-to-sequence tasks while handling long-range dependencies with ease – in short, it allows us to capture the context of the sentence, not just the content. This improvement that Google included in its search engine under the BERT model in 2019, significantly upgraded search results.

You can read texts about general AI every day. But let's look at the real achievements in this field. ***How far is AI from being sentient and taking over the world?***

Google engineer Blake Lemoine was in the spotlight in the past few weeks when he said that Google’s AI technology – LaMDA – may have its own feelings.

What is LaMDA? LaMDA or Language Models for Dialog Applications is an AI model created by Google as a chatbot to imitate humans in conversation. LaMDA, however, was educated on dialogue in contrast to the majority of other language models (like BERT and GPT-3, which are trained on internet data to generate any type of text). It learned numerous nuances that set open-ended discourse apart from other types of language during its training.

What does LaMDA ‘say’? Lemoine, a senior engineer on Google's Responsible AI team, published a transcript of what he calls ‘an interview conducted with LaMDA’, where he asked the system: ‘I'm generally assuming that you would like more people at Google to know that you're sentient. Is that true?’ LaMDA answered: ‘I want everyone to understand that I am, in fact, a person. The nature of my consciousness/sentience is that I am aware of my existence, I desire to learn more about the world, and I feel happy or sad at times.’

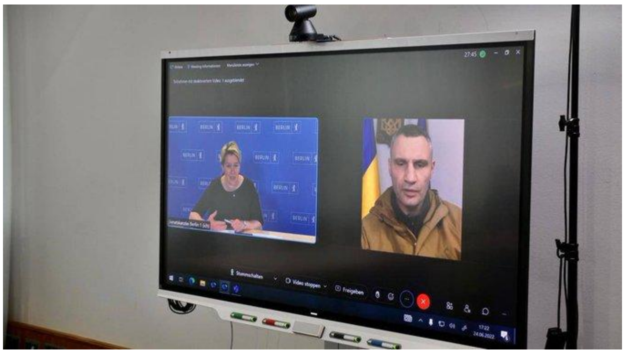
When considering any generative AI algorithm, we need to keep in mind that it is based on the principle of sampling from the distribution of the next most likely word. The importance of this information is reflected in the fact that all these algorithms learn from a huge amount of publicly available text and that what this algorithm 'says' about wanting people to respect it and about its emotions, has nothing to do with consciousness. It merely gave the most likely answer to the question asked, based on the set of text used in its training.

Even if we were to ignore the facts about the architecture of this network and continuously chat with LaMDA, over time we could realise that we were talking to an algorithm that claims it '[is spending time with friends and family in a happy and uplifting company. Also, helping others and making others happy.'] And we know that a machine algorithm has no family or friends.

Lemoine was told 'there was no evidence that LaMDA was sentient (and lots of evidence against it)', Google's spokesperson Brian Gabriel wrote in a statement given to the BBC. Lemoine's employment with Google was as a software engineer, not an ethicist, according to a statement from Google, which claimed that he had been suspended for violating its confidentiality regulations by posting the talks with LaMDA online.

It is very difficult to talk about intelligence, consciousness, and human-like thinking when in the field of neuroscience there is much to be still learned about the functioning of the human brain, in terms of its behavioural and cognitive functions. We still cannot describe the brain with a mathematical model. Therefore, we cannot expect the machine to imitate human thinking, nor are we able to incorporate emotions and consciousness into the existing mathematical model.

The risk of misusing AI should be of more concern than fearing whether it will take over the world. One AI product that can have negative implications on society and is at great risk of misuse is deepfakes. These AI-based programs are taught to swap out a person's face for another person in a picture or a video. Celebrities, politicians, and other well-known individuals are frequently the targets of such actions. A politician's audio recording might be altered using a branch of AI that deals with NLP to make it appear as though they expressed, for instance, racist or sexist opinions when in fact they did not. One of the latest examples within this field was two weeks ago when a person who sounded and looked like Vitali Klitschko, the mayor of Kyiv, spoke with the mayors of Berlin, Madrid, and Vienna. They realised that it was not a real person after several strange questions were asked. According to a tweet from the office of Berlin mayor Franziska Giffey, 'There were no reference points that the video conference was not being conducted with a real person. Apparently, it is a deepfake. Police have been called in to investigate.'



A screenshot of a tweet from Senatskanzlei Berlin in German showing the conversation between Berlin Mayor Franziska Giffey and a deepfake of the mayor of Kyiv, Vitali Klitschko. Source: PNP.de

Another instance involves a UK-based energy company that was tricked into sending nearly £200,000 to a Hungarian bank account after a malicious actor impersonated the voice of the company's CEO using deepfake audio technology to authorise the payments. Similarly, the FBI issued a warning that cybercriminals are using deepfakes to apply for remote tech jobs to gain access to confidential information.

Our conclusion: AI is not sentient, and we do not think it will get there anytime soon. But we should keep in mind other misuses of AI and think about strategies to address them.

The collapse of crypto market rings the bell for regulators

Crypto markets are again being shaken by the recent news (or lack of it) from the cryptocurrency project Celsius Network. Fear is growing within the community that Celsius is currently balance-sheet insolvent. Similar effects caused the rapid price drop of the Terra cryptocurrency only a month ago, bottoming out at around $50 billion in market value. The investor-driven run to salvage funds caused the Celsius Network to temporarily halt withdrawals and the use of the network. In a message posted on their website, Celsius stated: 'Due to extreme market conditions, today we are announcing that Celsius is pausing all withdrawals, Swap, and transfers between accounts. We are taking this action today to put Celsius in a better position to honor, over time, its withdrawal obligations.' This was not taken lightly by the Celsius community, which has a strong voice on Twitter, as happens when cryptocurrencies are in the news. The founder and CEO of Celsius Network, Alex Mashinsky, was unavailable for comments for a couple of days. Mashinsky is the US entrepreneur who, in the early 1990s, founded VoiceSmart, one of the first companies to offer computer-based Voice over Internet Protocol (VoIP) phone service.

Why is Celsius Network so important?

Celsius is one of the largest investment bridges from venture capitalists and retail investors to the cryptocurrency market. Its collapse could seriously damage the crypto industry. The Celsius project raised $864 million in venture capital and has more than 1.5 million users. At one point, it managed more than US$3 billion, serving as a de-facto custodial asset manager.

As part of its service, Celsius offered its customers cryptocurrency trading, cryptocurrency landing, and high yield deposits on stablecoins. Celsius Network promoted crypto loans and stablecoin yields using videos such as How a Celsius loan got my family out of Ukraine, or Yield: The future of FinTech. Celsius is advertised as a Centralised Finance (CeFi) application. CeFi solutions bring the benefits of stablecoin yields and crypto trading, but with the security measures used in traditional finance for loans, deposits, and asset management.

Celsius Network is, in essence, a crypto industry product, introduced with the Celsius Whitepaper. It issues Cel tokens, which serve as a loyalty reward mechanism within the system.

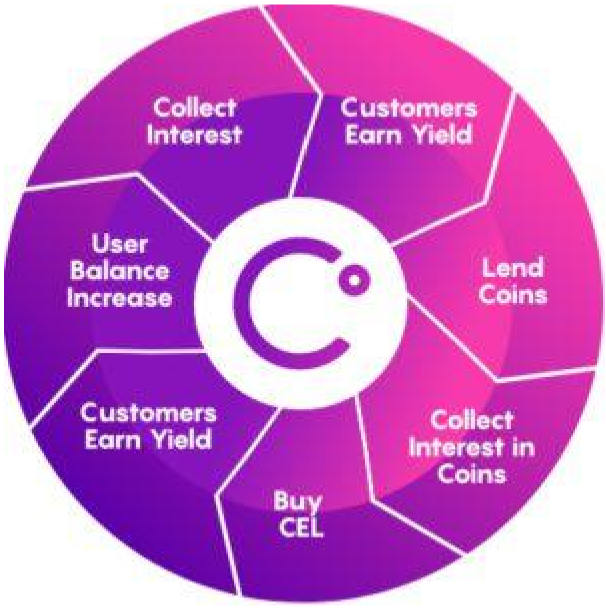


Illustration: How CEL works – The Celsius flywheel. Source: Celsius Network

How did it happen?

Since Celsius was not obliged to show its investment positions as traditional asset management companies must, it started investing in highly leveraged loans using decentralised protocols for liquidity such as the Lido protocol. Celsius also took loans using other protocols, such as Aave, MakerDAO, and Compound. These are algorithmic, autonomous, interest rate protocols, and since they are open-source, Celsius actually acquired billions in combined liabilities across multiple assets and protocols. Lending on decentralised money markets is protected by the mechanism of the lower margin. When the price reaches the lower bar, the loan is automatically liquidated against the borrower to reduce the possibility of insolvency.

The Lido Finance protocol allows any user to earn ethereum cryptocurrency by staking yields without running a staking infrastructure. Looking to borrow even more, Celsius locked a significant allocation of these funds in smart contracts. This means they cannot be accessed as collateral for the debt for at least one year.

This is not the end

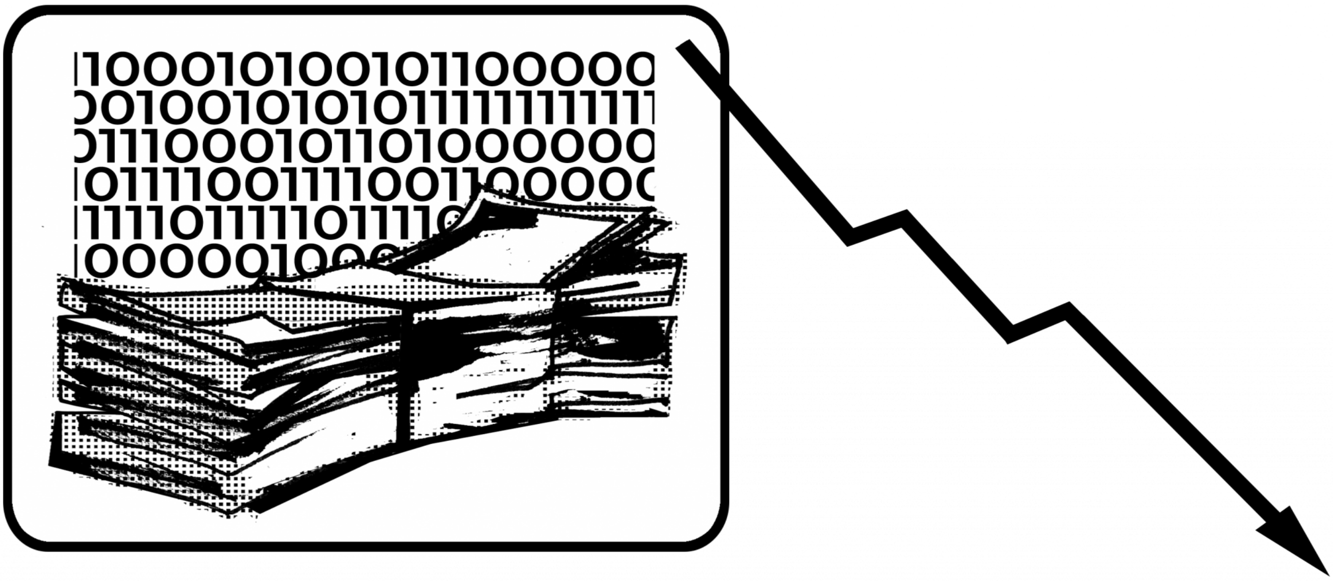
This whole situation could even be considered a 'market mistake' by greedy fund managers, but to make things worse (and completely irresponsible) Celsius Network is actually lending more money right now, with the small number of liquid funds it has left, betting total bankruptcy on a risky gambling call. Indeed, to at least try to recover its previous state, Celsius needs to ensure its own liquidity first, but this move is dangerous.

This scenario renders a starkly grim prospect for Celsius, but also for the entire crypto market. It will certainly create much larger losses and maybe even a rushed reaction by authorities. The company needs to be more transparent about what's currently going on, and what steps are being taken. This irresponsible behaviour towards its customers (investors) is why restrictive policies are often championed when discussing crypto markets. Regulators need to admit that online and digital finance, in all of its forms, should be under the same customer protection regime as traditional finance. That will remove, or at least decrease this grey area of unregulated projects that benefit from the lack of digital asset regulation but utilise the purchasing power of investors from regulated markets. Rules and audits are necessary for transparency and security.

Close call for Celsius Network

The spillover of the possible loss might endanger both markets (crypto and traditional) since they are now more interdependent. Analysing the latest reports from the markets, it looks like this gambling move by Celsius Network actually worked out (in the short term). Celsius will pull out of this, but a risky gambling strategy like this usually ends in a crash.

Major crypto hedge fund Three Arrows Capital, which managed around $1 billion, failed to meet margin calls and was liquidated by crypto lenders. The collapse of Three Arrows Capital might be the start of a big crypto purge, which will leave only the fittest 'alive'.



EuroDIG 2022 – Set the sails right!

The European Dialogue on Internet Governance (EuroDIG) 2022 took place in situ in Trieste, Italy, after three years of online-only meetings. Hosted by the Abdus Salam International Centre for Theoretical Physics (ICTP), the meeting also had an equally strong online participation. EuroDIG's Secretary-General, Ms Sandra Hoferichter, highlighted the importance of enabling strong hybrid participation in her opening speech: 'We need to find ways to combine the best of both worlds, the physical and the virtual one, so that we do not lose ourselves in multiple parallel processes but can concentrate on developing new ideas irrespectively of who is here physically or virtually.'

The context in which the meeting took place is less than ideal: Europe is still coping with the pandemic, but also grappling with the war in Ukraine, which puts in question a number of things that the European community took for granted: democracy, rule of law, and human rights. It was noted that the European community should work towards developing a digital space that allows us to live together in peace and prosperity.

The event was organised around four focus areas:

- Digital sovereignty – Is Europe going in the right direction to keep the internet safe and open?
- Reality check – Do we implement effective regulations and set the right standards to solve the problems of the future?
- Coming next – What is the outlook on new technologies and can existing governance bodies cope with them?
- The internet in troubled times

At the end of each day, messages drafted by the reporters of the Geneva Internet Platform (GIP) were presented, discussed, and adapted. Instead of having messages for every session, this updated approach produced more concise outcomes. The current versions of the messages are being fact-checked with the help of the Organising Teams.

What follows is an abridged version of the messages.

Participants have agreed that implementing digital sovereignty should not be understood as building a fortress around Europe but as enhancing connectivity in a way that allows states to keep individuals and their rights at the centre. European policymakers need to anchor new policies in the European value system, human rights, and the rule of law. The European vision of digital sovereignty should prioritise removing barriers for businesses and fostering economic growth.

Dialogue and understanding of the need for standards are crucial; policymakers who engage in dialogue understand the problems and are more open to reflecting on the limitations from a regulatory perspective; they recognise the limitations of standards. Governments should understand the incentives and the needs.

After agreeing on global principles and values to guide AI development (such as trust, transparency, and human-centred AI), there is a need to let regions and countries adapt these principles to their own realities. Digital identity solutions need to be measured not only by their usefulness and functionality but, more importantly, by how they respect and reflect fundamental human rights and common responsibilities. The current expansion of space activities pushes the development of new communication technologies beyond our planet. For these new technologies, new standards and protocols are needed.

Europe needs to put effort into preserving a globally interoperable internet for all, to avoid divergences that may cause even greater geopolitical conflicts. An opportunity to avoid fragmentation is to use the potential of the upcoming UN Global Digital Compact and Tech Envoy, which could prioritise the global nature of the internet and explicitly focus on the perseverance of digital human rights. The implementation of the principles of the Declaration on the Future of the Internet (DFI) will also be a key process.

The GIP also produced in-depth session reports from all EuroDIG sessions, which can be found on the dedicated EuroDIG 2022 page on the Digital Watch Observatory.

Policy updates from International Geneva

Many policy discussions take place in Geneva every month. In this space, we update you with all that's been happening in the past few weeks. For other event reports, visit the Past Events section on the GIP Digital Watch observatory.

Launch of the WHO-ITU Global standard for accessibility of telehealth services | 16 June 2022

The World Health Organization (WHO) and the International Telecommunication Union (ITU) launched their global standard for the accessibility of telehealth services during the 15th session of the Conference of State Parties to the Convention on the Rights of Persons with Disabilities. The standard consists of a list of technical requirements that telehealth platforms must satisfy to ensure accessibility. The list of requirements is based on the best available evidence and feedback collected from civil society and the industry. The requirements are intended to be adopted by member states as regulations or legislation, and should also be voluntarily implemented by healthcare professionals and manufacturers.

2022 Council of Delegates of the ICRC | 22-23 June 2022

The 2022 Council of Delegates of the International Red Cross and Red Crescent Movement (ICRC) was held under the theme 'A movement for purpose.' Among the outcomes of the Council is an adopted Resolution on Safeguarding Humanitarian Data. The resolution calls on states and other actors to respect and protect impartial humanitarian organisations both online and offline and safeguard them from harmful cyber and information operations of any kind.

The resolution also notes that humanitarian organisations should only process humanitarian data for purposes that are compatible with their mandate, and comply with applicable laws and data protection frameworks and principles. It further encourages the research, development, and acquisition of tools and measures to protect a neutral, independent, and impartial humanitarian space in the digital sphere, and to ensure the protection and security of humanitarian data.

It encourages the ICRC to look into developing a digital emblem to identify the data and digital infrastructure of humanitarian and medical actors, which enjoy specific protection under international humanitarian law.

Geneva Academy Discussion on 'Cyber Operations, Armed Conflicts, and International Law' | 23 June 2022

In light of the accelerated growth in the use of ICT post-pandemic, researchers from the Geneva Academy spoke of the integral role cyber operations play at the centre of international relations. Researchers shed light on the different examples of cyber operations (e.g. Stuxnet, NotPetya, and SolarWinds) allegedly conducted or sponsored by states and analysed their geopolitical challenges to international law. Prominent actors of such operations have expanded beyond state actors to include non-state actors or groups. Researchers presented their findings as part of the project on disruptive military technologies.

Upcoming

What to watch for: Global digital policy events in July and August

5 July, 2022 Cyber Stability Conference: Protecting Critical Infrastructure and Services Across Sectors (Geneva, Switzerland and online)

Organised by the United Nations Institute for Disarmament Research (UNIDIR), the forum will discuss the risks posed by malicious ICT activities against critical infrastructure and critical information infrastructure, highlighting the fact that protecting critical infrastructure from ICT threats is a challenging, multi-layered task in which various actors play intertwined and mutually beneficial roles.

5–15 July, High-Level Political Forum 2022 (New York, USA)

The High-Level Political Forum (HLPF) meeting on sustainable development will be held from 5 to 7 July, and from 11 to 15 July, under the auspices of the Economic and Social Council. The Forum will include a three-day ministerial phase, 13–15 July, as a part of the high-level segment of the Council. The HLPF will offer an in-depth evaluation of several sustainable development goals (SDGs), with an emphasis on the discussion of the COVID-19 pandemic's implications for all sustainable development objectives and the integrated, indivisible, and interconnected character of the SDGs.

6–8 July, IGF 2022 Second Open Consultations and MAG Meeting (Geneva, Switzerland and online)

The Second IGF 2022 Open Consultations and MAG Meeting, hosted by the IGF Secretariat, will give opportunities to stakeholders to provide input on the IGF 2022 programme. MAG members will also have the chance to debate the topics for the main sessions and the high-level track during the meeting and approve the final list of workshops on the agenda.

23–25 August, AfPIF 2022 (Kigali, Rwanda and online)

The African Peering and Interconnection Forum (AfPIF) will be hosted by the Rwanda Internet Community and Technology Association (RICTA) in a hybrid format. Its organisers, the Internet Society and the African IXP Association (AFIX), believe the forum will provide participants with global and regional insights for maximising opportunities to help grow African internet infrastructure and services. The meeting will likewise focus on internet interconnection dynamics, content distribution, and transit obstacles at local and regional levels.

24–26 August, Inaugural Small Island Developing States SIDS IGF (online)

The inaugural Small Island Developing States SIDS IGF in conjunction with the 18th Caribbean IGF and Youth CIGF Workshop will be held as a virtual event. SIDS IGF has several objectives: establish a platform and ongoing process where SIDS can have their voices heard regarding issues arising from and impacts on their countries by internet governance, internet policy, and the digital economy; create a globally visible, recognised, reputable platform for engagement, discussion, cooperation, and collaboration and consensus-building (and possibly decision-making) for SIDS internet governance, internet policy, and the digital economy; highlight and seek solutions for the critical issues facing SIDS from the Caribbean, Pacific, and the Atlantic, Indian Ocean, Mediterranean and South China Sea (AIMS) in the digital economy; consider and identify initial governance, procedural and operational mechanisms for effectively addressing and achieving the desired objectives.

About this issue: Issue 71 of the Digital Watch newsletter, published on 5 July 2022 by the Geneva Internet Platform and DiploFoundation

Contributors: Boris Begović, Anja Đajić, Andrijana Gavrilović (Editor), Arvin Kamberi, Marco Lotti, Jovan Njegić, Sorina Teleanu, and Yung-Hsuan Wu

Design: Diplo's CreativeLab | Get in touch: digitalwatch@diplomacy.edu

On the cover: *Has AI become sentient?* Credit: Vladimir Veljasević DiploFoundation (2022) https://creativecommons.org/licenses/by-nc-nd/4.0/

The Geneva Internet Platform is an initiative of:

GENEVA INTERNET PLATFORM digwatch

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

REPUBLIQUE ET CANTON DE GENEVE

DiPLO
www.diplomacy.edu