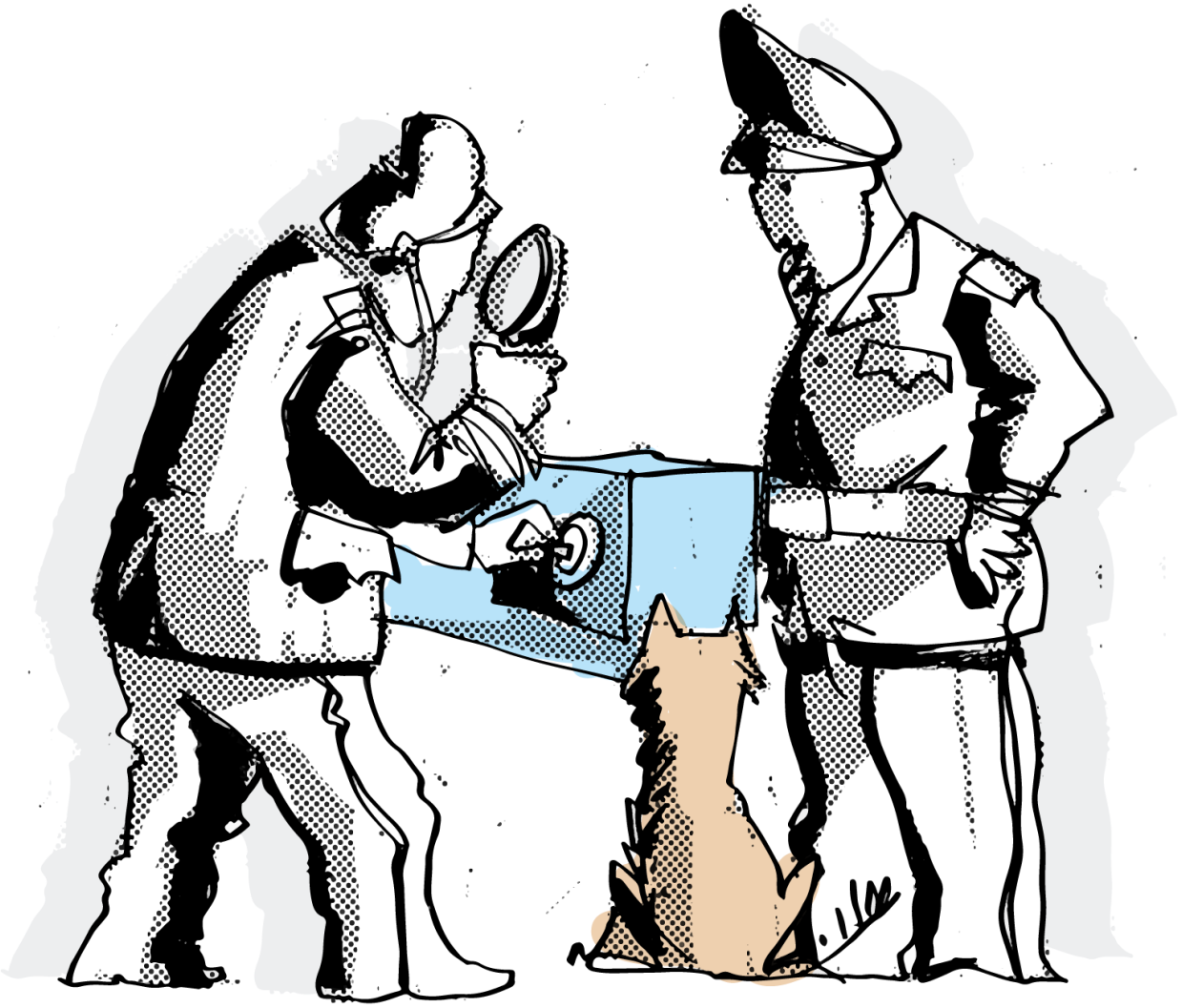
GENEVA INTERNET PLATFORM
digwatch

NEWSLETTER

Issue 74, **November 2022**



The battle for chips self-sufficiency

Pages 6–7

TRENDING

The battle for chips self-sufficiency, antitrust actions, and cyber (in)security trended in October.

Pages 2-3

LEGAL

The implementation of the Trans-Atlantic Data Privacy Framework is a new step forward for US-EU personal data flows.

Page 8

REFLECTIONS

Digital Cooperation Day (Geneva) tackled critical policy challenges and opportunities that the UNSG Tech Envoy must address.

Page 10

GENEVA

Diplo is turning 20 this month! We are celebrating this milestone with a series of events in Geneva, Malta, and online.

Page 11

Top digital policy trends

1. The battle for chips self-sufficiency

The USA is aiming to cut China off from certain semiconductor chips made anywhere in the world with US equipment, in an effort to slow Beijing's technological and military advances. To that effect, the Biden administration published a set of export controls regarding advanced computing and semiconductor manufacturing items on 7 October.

This move figures in the broader context of US plans to become independent in the chip manufacturing sector. The country has previously instituted the CHIPS and Science act, which intends to boost American semiconductor research, development, and production. This was followed by pledges for investment in the US chip manufacturing by companies like Taiwan Semiconductor Manufacturing Company (TSMC), Micron, Qualcomm, and Intel.

As for China, achieving self-sufficiency in their chip industry remains a key policy priority. The country strongly opposed the US export controls on semiconductor chips and called for their immediate abolition, the commerce ministry stated. China added that this decision by the USA not only hurts Chinese companies, but the commercial interests of US exporters, as well.

In midst of the tensions with the USA and a shortage of chips, China's chip imports market continues to decline.

Which actors are affected by these restrictions? What does each side gain or lose from this? How can it impact the global semiconductor supply chain? *Head to the In focus section on pages 6 and 7 for more.*

2. Antitrust authorities flex their muscles

Antitrust authorities are tightening measures against tech companies with the aim of promoting stronger competition in digital markets. This month, Google, Amazon, Meta, and the South Korean KakaoTalk hit the headlines.

Google is under pressure in Asia, as well as in Western economies. In India, an ongoing probe on Android, conducted by the Competition Commission of India (CCI), concluded that Google leveraged its dominant position in the Android App Store to protect its own apps, such as Chrome and YouTube. According to CCI, Google should give individuals the option to use the search engine of their choice and uninstall the pre-installed apps like Google Maps and Gmail. In the EU, the Commission appears to be gearing towards a heavy fine early next year on Google's ad tech business, over an alleged unfair advantage it gives to Google over rivals and other advertisers. The company may still avert the billion-euro fine and settle the investigation if it offers enough concessions and remedies.

In the UK, the Competition and Markets Authority (CMA) won an arm wrestling match with Meta over the acquisition of Giphy. In 2021, the UK regulator ordered Meta to reverse the deal over concerns with the impact that the acquisition could have on competition and innovation. Meta announced that it will sell Giphy and comply with the CMA's order, following an unsuccessful appeal. Amazon is expected to face a class action lawsuit over allegations that the algorithms behind its 'Buy Box' feature – a coveted spot that makes items more visible to shoppers – favours Amazon's own products and those of third-party sellers who use Amazon's storage and delivery services.

In South Korea, a major outage left KakaoTalk – the country's main messaging app – unavailable. The disruption was compared to a failure of the national communications network by president Yoon Suk-yeol. KakaoTalk is heavily relied on for a wide range of activities, from online payments and ride hailing, to providing log-in verification for third-party websites. The outage prompted a discussion on whether the company holds a potentially dangerous monopolistic position.

Amidst the tightening of oversight, not everything is doom and gloom for tech companies. In Italy, an administrative court in the Lazio region overruled a decision from the Italian competition authority that imposed fines on Apple and Amazon. The decision concerned a clause in the 2018 contract concluded

between the two companies that allegedly granted Apple Premium Resellers a privileged position for selling Apple's earplugs on Amazon's marketplace. Substantive and procedural reasons were argued by the judges of Lazio to justify their decision. According to them, the competition authority failed to provide sufficient evidence, and the two companies were not given enough time to defend themselves.

3. Cyber(in)security

An unusually high volume of cyberattacks was noted in October 2022. Neither companies nor countries were spared.

At the very beginning of the month, telecommunications company Optus revealed that the September cyberattack the company suffered has exposed personal information of 2.1 million customers. On the heels of this bleak news, just a day later, another cyberattack hit Australia's telecoms sector. This time the target was Telstra, and customers' data remained safe – it was Telstra's staff whose names and email addresses were published online. Cyberattacks on entities in the continent continued with the hack of one of the biggest health insurers, Medibank, during which the personal data of 3.9 million of Medibank's customers was accessed by the hackers. The data includes personal information such as names, dates of birth, addresses, and gender identities, as well as Medicare numbers and health claims, Medibank disclosed.

Home Affairs Minister Clare O'Neil said Australia needs to reform its cybersecurity laws to give the government stronger powers to respond to cybersecurity emergency incidents. A proposed change in the country's privacy rules is already in the works: the maximum penalties that can be applied for serious and repeated privacy breaches will be increased, and the powers of the Australian Information Commissioner and the Australian Communications and Media Authority strengthened. For instance, the Commissioner will get greater powers to address privacy breaches, while both institutions will have greater information sharing powers.

Companies elsewhere have suffered data breaches as well. Hackers breached an undisclosed amount of prepaid Verizon accounts, potentially accessing names, telephone numbers, billing addresses, price plans, and other service-related information on compromised accounts. Surfshark says that a total of 108.9M accounts were breached worldwide in 2022'Q3 (July, August, September), which is 70% higher than in Q2. Looking at October only, we have an inkling the numbers for Q4 won't be much better.

Ransomware has not quieted down. One of India's largest electricity producers, Tata Power, suffered a ransomware attack which reportedly exposed personally identifiable information (PII) like Aadhaar national identity card numbers, tax account numbers, salary information, addresses, and phone numbers, among others. Microsoft identified a new ransomware called 'Prestige,' targeting Ukrainian and Polish transport and logistics companies.

Even REvil seems to be back in the game – researchers at Palo Alto have linked Ransom Cartel ransomware to REvil ransomware. Australia's woes continued with a ransomware attack on the national defence communications platform, although it seems that no data has been breached.

Other governments faced cyberattacks too. Saudi Government Portal, Absher, was targeted in a new phishing campaign aiming to take data from Saudi citizens. Iran's atomic energy organisation reported that one of its email servers was hacked, and has attributed the attack to a foreign country, even though an Iranian hacktivist group claimed responsibility for it earlier. The parliament of Poland suffered a cyberattack, the attack being described as 'was multi-directional, including from inside the Russian Federation,' according to the Polish Senate speaker. Also, targeted this month were Bulgaria and the USA, in both cases by DDoS attacks reportedly by Russian hackers. Bulgarian government institutions, including the Internal Affairs Ministry, the Defence Ministry, and the Justice Ministry, were hit. In the USA, government websites in multiple states were knocked offline, hacking group Killnet taking responsibility.

What seems to be needed is more than the usual calls for cooperation on cybercrime and pledges for responsible behaviour in cyberspace.

Digital policy developments that made headlines

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

Same relevance

Global digital governance architecture

The International Telecommunication Union's (ITU's) Plenipotentiary Conference concluded with agreements on a wide range of issues, from ICT and climate change, to AI and outer space.

The European Commission's work programme for 2023 includes plans for a critical raw materials act, a common European mobility data space, and tools for open human-centric virtual worlds, among other issues.

China reiterated plans to achieve self-reliance in technology.

Same relevance

Sustainable development

The European Commission published guidelines for teachers on promoting digital literacy.

The Science and Innovation Forum of the UN Food and Agriculture Organization highlighted the role of technology and digitalisation in the transformation of agrifood systems.

Increasing relevance

Security

Wholesale giant METRO confirmed it was a victim of a cyberattack, which caused partial IT infrastructure outages. Europe's biggest copper smelter, Aurubis, suffered a cyberattack that forced it to shut down its IT systems as a preventive measure. *Read more about security in October on page 3*.

Increasing relevance

E-commerce and the internet economy

The Financial Stability Board proposed a framework for the international regulation of crypto-asset activities. South Africa requires cryptocurrency companies to apply for licences in 2023. SWIFT experiments show that central bank digital currencies and tokenised assets can move seamlessly on existing financial infrastructure.

EU and US competition authorities agreed to continue collaboration in the technology sector. *Read more about the internet economy in October on page 2.*

Same relevance

Infrastructure

Damages to internet cables in France and the UK caused connectivity disruptions. The European Commission proposes a recommendation on strengthening the resilience of critical infrastructure.

The Body of European Regulators for Electronic Communications raised concerns over Commission's plans to require platforms to pay for telecom infrastructures.

Increasing relevance

Digital rights

The US president signed an executive order on safeguards for intelligence activities, paving the way to a new EU-US data privacy framework. *Read more in the Legal section on page 8*.

The attorney general of Texas, USA, sued Google for allegedly using biometric data without proper consent. TikTok denies allegations that its parent company has plans to use the map to monitor the location of certain American citizens.

The Court of Justice of the European Union issued its judgement in Case C-129/21 | Proximus (Public electronic directories) stating that the controller of personal data under the GDPR is obliged to inform other controllers should the data subject withdraw his or her consent.

Same relevance

Content policy

Turkey passes a law that imposes criminal penalties for the spread of false or misleading information.

Facebook says it may block the sharing of news content in Canada if legislation is passed requiring platforms to pay news publishers.

Having completed the acquisition of Twitter, Elon Musk intends to introduce a moderation council, something on verification of users, and reboot video app Vine.

Increasing relevance

Jurisdiction and legal issues

A Brazilian court fines Apple and rules that iPhones must be sold together with chargers. *Read more about legal issues in October on page 2*.

Technologies

IBM announced plans to develop a chip specialised for AI.

The US White House publishes a blueprint for an AI bill of rights.
NATO establishes a review board to govern the responsible use of AI. The European Commission issues guidelines for teachers on the use of AI.

The Czech Republic, France, Germany, Italy, Poland, and Spain were selected to host future European quantum computers.

Increasing relevance

The battle for chips self-sufficiency

The US government introduced new controls on exports of advanced computing and semiconductor manufacturing items to China, in a bid to prevent China from purchasing and manufacturing certain high-end chips.

'*The PRC has poured resources into developing supercomputing capabilities and seeks to become a world leader in artificial intelligence by 2030. It is using these capabilities to monitor, track, and surveil their own citizens, and fuel its military modernization*,' Assistant Secretary of Commerce for Export Administration Thea D. Rozman Kendler stated. '*Our actions will protect U.S. national security and foreign policy interests while also sending a clear message that U.S. technological leadership is about values as well as innovation.*'

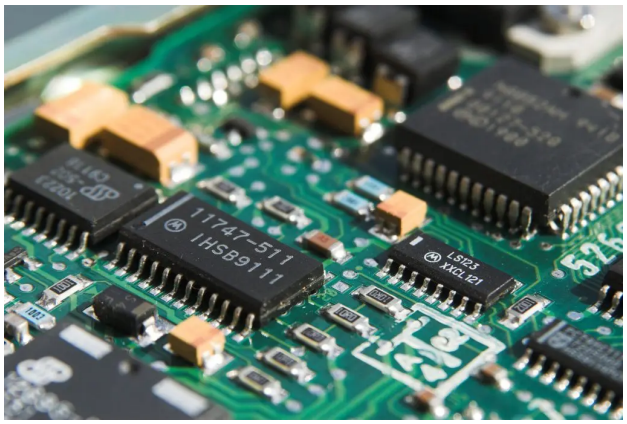


Image credit: Axonite/Pixabay

What does that mean?

This means that the October 7 measures **prevent US firms from selling advanced chips to China** *or* **providing Chinese firms with tools for making their own advanced chips**. They also **prevent firms from other countries from doing the same**, if those chips or tools were made with US-made technologies. There isn't almost any semiconductor without some kind of US-trademark bits in its design or production process.

The rules also **prohibit US citizens** from participating in, or facilitating activities, that encourage the development or manufacture of specific integrated circuits (ICs) at Chinese fabrication facilities.

How are trade restrictions put in place?

This is achieved by adding certain semiconductor manufacturing equipment, advanced chips, and commodities containing such chips to the Commerce Control List ('CCL') of the Export Administration Regulations ('EAR'). The scope of items being subject to the EAR was substantially expanded.

New licence requirements for certain items from the USA destined for China have been added. Companies can apply for a licence to export, re-export, or transfer (in-country) items. The applications will be evaluated on a case-by-case basis by the US Department of Commerce, taking into account the technological level, clients, and compliance plans.

The ban affects the most advanced chip technology available, while older and less developed chip technologies are not targeted by the ban.

How does this affect China?

China's main role in the chip supply chain is that of a vast consumer of semiconductors, importing a sizable percentage of the chips they use. Figures from the National Bureau of Statistics of China note that the country has imported about 47.6 billion chips in September 2022. To illustrate further, China accounts for 33% of sales at Applied Materials, 27% at Intel, and 31% at Lam Research. The new US export licence requirements aim to restrict China's access to the most advanced chip technology.

Chinese chipmakers will be affected, as well. The US Bureau of Industry and Security has added 31 of such companies to an 'unverified list', making Chinese chipmakers ineligible to receive items subject to the US government's export regulations. For example, China's top chipmaker Semiconductor Manufacturing International Corporation (SMIC), will be affected by the US restrictions mainly in areas of maintenance and equipment replacement.

This will also affect companies such as Yangtze Memory Technologies Corp and ChangXin Memory Technologies, because they produce advanced products which require the chips which fall under the ban. In addition, the

USA has cut off US citizens – employees and talent – from the Chinese chip product development sector without a proper licence. YMTC asked American employees in core positions to leave the company in order to comply with the export controls. Naura Technology has already asked its US engineers to stop working on R&D projects, effective immediately.

What are the reactions from China?

It is not surprising that China has strongly opposed the new US rules. China's foreign ministry spokesperson Mao Ning said: '*In order to maintain its sci-tech hegemony, the US has been abusing export control measures to wantonly block and hobble Chinese enterprises. Such practice runs counter to the principle of fair competition and international trade rules. It will not only harm Chinese companies' legitimate rights and interests, but also hurt the interests of US companies. It will hinder international sci-tech exchange and trade cooperation, and deal a blow to global industrial and supply chains and world economic recovery.*'

China's top trade group for the chip sector, China Semiconductor Industry Association (CSIA), warned that the export controls could put more stress on global supply chains. Research labs and commercial data centres could be denied access to advanced AI chips, Chinese chip fabs could not purchase critical manufacturing equipment, and US nationals working for advanced Chinese chip companies would be forced to resign.

A law passed by China in 2021 allows countermeasures against sanctions. Despite Washington's tightening semiconductor controls, it has not yet been used. However, sanctions and counter-sanctions bring the possibility of hurting consumers in both countries and beyond.

What's the effect on the global supply chain?

The USA is home to the majority of chip design companies, such as Qualcomm, Broadcom, Nvidia, and AMD. US companies are leaders in the production of equipment used for the production of semiconductors, with 31% of the turnover, closely followed by European ones, such as ASML, with 27%. Taiwanese and South Korean companies dominate in the manufacturing part of the chipmaking process – Taiwan-based TSMC produces over 50% of chips worldwide, while South Korean companies SK Hynix and Samsung together control about 70% of the smartphone chip market. All these companies will have to be certain that they comply with the export rules. Analysts note that semiconductor companies will incur billions of dollars in lost sales.

The USA has tried to soften the blow to the global economy by granting waivers. TSMC has been granted a one-year licence to continue buying American chip making equipment for its expansion in China. SK Hynix has also obtained authorisation from the USA to receive goods for its chip production facilities in China, without obtaining additional required licensing imposed by the new rules. Samsung Electronics Co has reportedly been granted a one-year exemption allowing it to continue receiving chip making equipment and other items needed to maintain its memory-chip production. Intel received a one-year authorisation to continue its current NAND memory chip operations in Dalian, China.

Who will win the battle?

Can there be a winner, at all? It's too early to tell.

The USA will try to ink a deal with allies to support the new rules in the near-term, Under Secretary of Commerce for Industry and Security Alan Estevez stated. Taiwan's Economy Ministry has signalled that it will comply with the export controls. However, it is uncertain that Japanese and Dutch companies will be willing to do so.

China won't just give up its spot in this industry, moving to relying on their own production of chips. However, the rules could slow down the Chinese chip industry significantly, until it shifts to being self-sufficient. 'I think it will slow them down for two to five years, not 10', said Tudor Brown, a former independent director at SMIC. On the other hand, the rules could also significantly boost domestic semiconductor manufacturing in China. China's local governments have already started doubling down on cash incentives and policy support for domestic chipmakers.

Personal data transfers – new EU-US way forward

US President Biden recently issued an Executive Order to implement the Trans-Atlantic Data Privacy Framework announced in March 2022. The Executive Order aims to re-establish the legal regime enabling personal data to flow from the EU to the USA without any further safeguard being necessary under the General Data Protection Regulation (GDPR). In practice, this means that companies will finally have more peace-of-mind when moving personal data across the Atlantic.

This is coming after a two-year gap since a previous adequacy decision by the European Commission (EC) based on Privacy Shield was invalidated by the Court of Justice of the European Union (CJEU) in 2020 (Schrems II case).

The Executive Order addresses issues that led to the invalidation of the previous arrangement – such as the US intelligence personal data collection beyond necessary and proportionate, lack of oversight over such collection, and lack of binding redress for the EU citizens.

The Framework and the Executive Order set up the implementation of 'new safeguards to ensure that [sic] intelligence activities are necessary and proportionate', and expand oversight and compliance in order to address concerns of overreach by the US intelligence.

To address the lack of redress by the EU citizens in cases of violation of their personal data rights, the Executive Order creates a 'multi-layer mechanism.' Individuals may submit complaints to the Director of National Intelligence's Civil Liberties Protection Officer (CLPO), who is obligated to investigate and remediate complaints. CLPO decisions are binding and subject to review and assessment by the independent Data Protection Review Court. The court will have the capacity to investigate complaints, including the right to request relevant information from intelligence services, and will have the ability to make legally enforceable rulings.

The Executive Order also instructs the Privacy and Civil Liberties Oversight Board, an independent agency within the executive branch of the US government, to examine and conduct an annual review of adherence to the redress decisions by the intelligence community.

What do the critics say?

While there is general praise for the progress on the EU-US personal data transfers, there are concerns about whether this legal framework will be sufficient. The concerns relate to:

- Doubts about the extent to which an executive order can be an effective legal instrument for implementing GDPR safeguards as the US legislature has not passed it. (see German DPA)
- Constitution of the Data Protection Review Court, as it is under the executive branch of government and not the judicial branch (voiced by the NOYB)
- The EU and US agreed on legal terminology for 'necessary' and 'proportionate' when it comes to surveillance, but not on its legal interpretation (as stated by NOYB and the German DPA)
- No substantial improvements in addressing issues related to the commercial use of personal data (voiced by the European consumer organisation)

What's next?

Now, it is the EU's turn to proceed. The EC will review and determine whether the Executive Order provides Europeans with adequate data privacy protection and draft a new adequacy decision.

The EC must then hear from the European Data Protection Board and the EU member states. However, while not bound by the board's opinion, the EC must consider it.

On the other hand, the EU's member states could block the agreement.

The formal adoption process for the adequacy decision by the EC is not expected not before the spring of 2023.

Digital Cooperation Day

The importance of Geneva for digital technologies and pertinent policymaking shone through on the Digital Cooperation Day. Distinguished guests and panellists convened to speak of critical policy challenges and opportunities that are to be tackled as part of the upcoming Global Digital Compact (GDC). The programme of the day included keynote messages, a presentation on the Geneva Internet Platform's (GIP) contributions to the Geneva digital landscape, a presentation on the GDC's visions by UN Secretary General's Envoy on Technology Amb. Amandeep Singh Gill, two panel discussions, and final takeaways.

In recent years, the transformative forces of digital technologies in economies, societies, and politics are not to be missed. The COVID-19 pandemic especially highlighted the costs of being digitally excluded. Ms Doreen Bogdan-Martin (Director, Development Bureau, International Telecommunication Union (ITU)), underlined that it is high time to aim for 'zero tolerance in digital exclusion'. Acknowledging the negative consequences we must mitigate, and the positive outcomes we must maximise in digital transformation, the keynote speakers elaborated on the role of Geneva and Switzerland in digital policy discussions and in advancing a digital cooperation agenda.

The panel discussions allowed for each expert, coming from various backgrounds, to give Gill a message on what needs to be achieved with the forthcoming GDC. Gill envisioned a transition from contemplating the 'what' and 'why' to 'how' we could substantiate digital cooperation. The key priority, as he pointed out, is to incorporate the voices of youths, the marginalised, and all those who are not already enjoying the digital ecosystem into the input for the ministerial and UNGA meetings in 2023 and the Summit of the Future in 2024. Gill challenged the participants to reflect upon the need to strengthen interlinkages among important digital policy stakeholders in Geneva. This puts into question whether there are missed opportunities for collaboration and whether digital policy actors could explore the building of new partnerships for dealing with cross-cutting digital issues.
Some key messages of the day included:

- The entrepreneurial community innovating new usage of digital technologies would need policy support which would ensure both monetary sources and clients for start-up companies. Governments could be not only the investors of those start-ups, but also their customers, harnessing the fact that start-ups are more in touch with rapid tech development on the ground and more willing to solve societal or SDG-related challenges than the big techs.
- In the discussion of digital cooperation, it must not be overlooked that different groups of states, due to population size, economic opportunities, etc., will inherently have different sets of issues in digital transformation. It is imperative for these different groups to work on common perspectives and languages through diplomatic means to voice out their needs.
- There seems to be a disconnection between civil society organisations and tech companies, despite the attempts by both sides to address the interlinkages between social issues and technological advancements. The UN Tech Envoy should provide a regularised platform where tech companies and the constituencies of International Geneva could exchange knowledge and expertise.
- After the COVID-19 pandemic, practitioners in some traditional political fields, such as mediation, have seen the merits of incorporating digital technologies in their operations. Hence, there is an urgency to develop international laws or soft laws to ensure the protection of involved parties and serve as guidelines for these fields of operations.
- In terms of building trust in digital technologies and their usage for social good, both the design of technological products and the regulatory environment in which these products are conceived must be taken into account.
- It is pressing for digital actors in Geneva to look for innovative ways to break silos and partner with each other in face of cross-cutting issues. Such partnerships could take more of an ad hoc, issue-by-issue basis due to the fast changing nature of digital topics.

Policy updates from International Geneva

Numerous policy discussions take place in Geneva every month. Here's what happened in October.

Building Bridges 2022 | 3–10 October

The Building Bridges joint initiative, since its launch in 2019, has been bringing together the Swiss public authorities, the finance community, the United Nations, and other international partners to collaboratively work on transitioning a global economic model aligned with the Sustainable Development Goals (SDGs). The 2022 edition saw high-level dialogues, 65 crowd-sourced events, and multiple networking events. Some highlights include the reaffirmation of Switzerland's preparedness for hosting the Conference of Parties (COP) in 2026 and the panel discussion with entrepreneurs on regulations around sustainable finance.

Geneva Science and Diplomacy Anticipation Summit 2022 | 12–14 October

The Geneva Science and Diplomacy Anticipator (GESDA) hosted its 2022 summit at Campus Biotech, Geneva, facilitating discussions around possibilities for collaborations and best practices for inclusive and responsible diplomacy. GESDA showcased this year's update on the Science Breakthrough Radar, which makes predictions on 40 emerging scientific trends in the next 5, 10, and 25 years. GESDA also presented the first prototypes of 'solution ideas', which propose potential avenues of actions enabled by these emerging trends.

Geneva Cybersecurity Forum: What are the challenges of cybersecurity in times of war and peace? | 13 October

The Geneva Press Club (Club suisse de la presse) and the CyberPeace Institute jointly hosted the in-person forum debate on actions needed against cybersecurity threats today and in the future. The titular question was explored under the backdrop of the COVID-19 pandemic, which has spurred the growth of online activities. Cyberattacks have grown more sophisticated and damaging to all economic actors. Nation states and civilian critical infrastructure are both falling victims. The first panel addressed the responsibilities of states to protect people against cyberattacks and the intricate relations between the public and private sectors. The second panel deliberated on the relevance of cyber weapons in 21st-century conflicts. Watch the recordings here.

2022 Annual Conference of the Geneva Human Rights Platform: On/off: Implications of digital connectivity on human rights | 18 October

The Conference turned to digital connectivity in the field of human rights, exploring how digitalisation could exert both positive and negative impacts. Issues tackled include the evolution of international human rights law in this digital area and the role of the Geneva-based international human rights (IHR) system to ensure the continuum of protection. The expert roundtable on digital human rights tracking tools brought together, for the first time, experts in the field to discuss the implementation of the IHR obligations and generated recommendations for accountability bodies.

Upcoming

The main digital policy events in November

3–18 November, IEEE World Forum on Internet of Things (Yokohama, Japan)

The 8th IEEE World Forum on Internet of Things will be held from 26 October to 18 November 2022 in Yokohama, Japan and online. The main theme of the forum is 'Sustainability and the Internet of Things', and the discussions will centre around the four pillars of sustainability: human, social, economic, and environmental. The World Forum will specifically focus on how technical IoT applications and solutions contribute to the seventeen Sustainable Development Goals that were developed in the UN Brundtland Report.

5–11 November, IETF 115 (London, UK)

The third and final IETF meeting of 2022, IETF 115, will be a hybrid meeting held in London, UK and online. As per usual, the community will gather to discuss network management, crypto, web authorisation protocols and other topics within the Internet standards scope of work. The agenda of the meeting is available. The IETF Hackathon and IETF Codesprint, as well as newcomers' training and technical tutorials will be held prior to the meeting.

15–16 November, G20 Summit (Bali, Indonesia)

The 17th G20 Heads of State and Government Summit will take place on 15 and 16 November 2022 in Bali. The G20 Summit under the presidency of Indonesia will come together to discuss the presidency's three priority issues: global health architecture, sustainable energy transition, and digital transformation. This year's topic is 'Recover together, recover stronger' from the consequences of COVID-19.

21–23 November, European Big Data Value Forum 2022 (Prague, Czech Republic)

European Big Data Value Forum is BDVA's flagship event, bringing the whole European data-driven AI research and innovation community together to share knowledge, collaborate, and celebrate achievements. This year's theme is 'At the heart of the Ecosystem for Data and AI'. The programme includes sessions that shape the way forward for data spaces, illuminate how businesses can harness the power of trustworthy AI, and discuss the role of HPC as an enabler for digital transformation. The topics are discussed from the perspective of all European sectors, focusing on smart cities, energy, healthcare, manufacturing, and automotive industries.

28–30 November, UN Forum on Business and Human Rights (Geneva, Switzerland)

The 11th UN Forum on Business and Human Rights will be held both online and at the Palace of Nations in Geneva, Switzerland. The theme of the Forum is 'Rights holders at the centre: Strengthening accountability to advance business respect for people and planet in the next decade'. The Forum, established in 2011 by the UN Human Rights Council, is the global platform for yearly stock-taking and lesson-sharing on efforts to implement the UN Guiding Principles on Business and Human Rights.

28 November–2 December, Internet Governance Forum 2022 **(Addis Ababa, Ethiopia and online)**

The 17th edition of the Internet Governance Forum (IGF) will be held under the overarching theme 'Resilient Internet for a Shared Sustainable and Common Future.' The programme is focused on five themes: Connecting All People and Safeguarding Human Rights, Avoiding Internet Fragmentation, Governing Data and Protecting Privacy, Enabling Safety, Security and Accountability, Addressing Advanced Technologies, including AI. The themes are drawn from the UN Secretary General's Global Digital Compact. The GIP will traditionally provide reports from the IGF, which will be available at the IGF 2022 dedicated page on the Digital Watch.

Upcoming

20th Diploversary

Diplo, the organisation behind Geneva Internet Platform (GIP) is celebrating its 20th birthday this year. Join us in this journey through a series of Diplo's 20th anniversary events!

Diplo Week in Geneva

Diplo Week in Geneva will feature a series of open-door events for participants to learn about cutting-edge AI applications and data analysis tools that Diplo has developed, as well as other exciting findings from Diplo's research factory.

Between 7 and 11 November, Diplo will focus on a different crucial theme pertinent to digital technologies each day: digital development and inclusion, AI and data management, humanitarian diplomacy, and cybersecurity. Diplo Week in Geneva also features:

- a pre-release presentation of Diplo's study *Stronger African Digital Voices*
- the official launch of the *Geneva Digital Atlas 2.0* which comprehensively maps out the digital policymaking and internet governance ecosystem in International Geneva
- opening of an art exhibition featuring the work of Prof. Vladimir Veljašević.

To learn more and register, visit the Diplo Week web page.

Summit on digital diplomacy and governance

Digital diplomacy and governance will be the focus of an international summit taking place on 17–19 November in Malta, as well as online.

Here's five reasons to join the summit, in person or online.

1. It will be a major gathering of tech envoys and digital policy experts from around the world.
2. We will think beyond traditional narratives and hype, and try to find new solutions for the new era.
3. We will dedicate a part of the programme to facilitate a consultation on the Global Digital Compact, the initiative launched by the UN Secretary General in 2021, which will be agreed upon at the UN Summit of the Future in 2024.
4. Africa holds a special place at the summit. We will launch our latest report, '*Stronger Digital Voices from Africa*', with insights on how Africa can build its digital foreign policy and diplomacy.
5. Last but not least, we will celebrate the 20th anniversary of Diplo!

To learn more and to register, visit the summit website.

Visit our dedicated page to learn more about our story and celebrate Diplo@20 with us!

About this issue: Issue 74 of the Digital Watch newsletter, published on 4 November 2022 by the Geneva Internet Platform and DiploFoundation
Contributors: Boris Begović, Stephanie Borg Psaila, Andrijana Gavrilović (Editor), Pavlina Ittelson, Marília Maciel, Jana Mišić, Anamarija Pavlović, Sorina Teleanu, and Yung-Hsuan Wu
Design: Diplo's CreativeLab | Get in touch: digitalwatch@diplomacy.edu
On the cover: *The battle for chip self-sufficiency?* Credit: Vladimir Veljasević DiploFoundation (2022)

The Geneva Internet Platform is an initiative of:
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
REPUBLIQUE ET CANTON DE GENEVE
Operated by:
DiPLO
www.diplomacy.edu