

Special: Digital policy in 2022

Pages 2–5

BAROMETER

What's hot, what's cold, and what's lukewarm? Our predictions have already started playing out, with prominent developments in security, e-commerce, and human rights.

Pages 6–7

DMA & DSA

It will be a critical year for the regulation of tech companies. Europe is moving fast with two pieces of legislation. Here's a recap, plus the latest updates.

Pages 8–9

STANDARDS

As digital standards gain more attention, our short guide provides the tools you need for navigating the policy space.

Pages 10–11

GENEVA

Many policy discussions take place in Geneva every month. January was no different. Read on for an update on what's been happening in International Geneva.

Page 12

The three trends that will shape digital policy in 2022

Three main trends will shape the way digital policy will unfold this year. The first is a tug-of-war between governments and companies for economic and political power. The second is a quest by states to assert sovereignty over what's perceived as the digital realm. The third is a need to protect our digital interdependence, that is, the way the internet has bound us all together.

1. A tug-of-war for economic and political power

It's usually good news for governments when a homegrown company is able to employ thousands of people, generate millions in economic activity, and invest some of it at home to improve infrastructure and critical assets.

There comes a point, however, when a company has grown so much in economic and political power that it harvests as much personal data as it can, takes out rival companies when it feels a threat, eliminates public figures from its social platforms, and decides the rules of the game for traders using its marketplace. This is the point when governments decide certain companies have grown too much.

Yet, if it were simple to reign in their power, governments would have already done so. And there's a lot at stake – from huge investments at every level of the economy and thousands of jobs and livelihoods to access to the technology people use to connect instantaneously with family and friends. Take any of that away, and governments are in deep trouble.

This tug-of-war for economic and political power will intensify this year as governments come under increasing pressure from other

sectors of the economy and other countries to regain power and influence. But there's a second battle...

2. A quest to assert (more) sovereignty

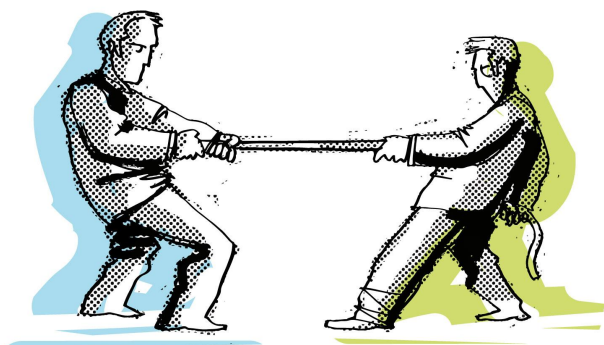
Sovereignty is the bedrock of any legitimate ruling system. It gives a government the authority to govern a country and uses geography (and in some cases nationality) to delineate the extent of its jurisdiction.

Geography is easy to gauge: Just look at a map. But the digital realm creates the perception that there is a parallel space that is devoid of geography. And if there's no geography, how can governments govern the digital realm?

Governments are quickly realising that the digital realm is, indeed, anchored in geography. The information we look up online, in the intangible cloud, is travelling through physical cables that span valleys, mountains, and oceans. The cloud is a network of data centres located in cities around the globe. If it's linked to geography, it can be ruled. As this realisation grows, so does the quest to rule digital activities and establish a flag of sovereignty over them.

For instance, some countries have taken a sovereign approach to governing people's data, and have ordered companies to store that data within the country's geographical borders. Others impose limits on the kind of information people can access online or through the internet, social media, or online games.

Despite a state's right to assert its sovereignty, some digital aspects require a wider understanding of the issues and a different governance approach.



3. A need to protect digital interdependence

The internet has transformed the world into a globalised society. In modern parlance, the internet has changed us into a continuously interconnected and interdependent community.

This is the world we've come to experience and appreciate. There's no going back from this instantaneous way of communicating and interacting. Without minimising the ugly side of the force, today's world of digital interdependence has brought many advantages (or digital dividends) for society. E-commerce can't really exist without access to sellers and customers from other markets. Data flows across borders are crucial for technological innovation. Without data, policymaking wouldn't be as informed as it is today. It follows that any decision or action that governments, companies, and citizens take should not break this interdependence.

In practice, this requires strong collaboration and cooperation. That's because we need to bring digital dividends to everyone and to contain the ugly side (data leaks and breaches, misinformation, violent extremism, surveillance, digital divide, and all kinds of risks and threats).

This will require some tough trade-offs on every digital policy issue you can think of – from antitrust and data protection to AI, emerging tech, and cyberconflict.

But perhaps the toughest decisions will emerge as governments and companies navigate the redistribution of economic and political power and in the quest for (more) sovereignty.

This article is based on 10 Digital Governance and Diplomacy Trends for 2022, published by Prof. Jovan Kurbalija. Read the full text [in English](#) and [in French](#).

Predicting 2022: What to expect on issues of security, human rights, and development

A. Peace and security

- Resilience: The possibility of a cyberattack crippling a country's critical resources rests heavily on governments' minds. Expect more attacks, but also more measures which deter.
- US-Russia: Expect more (but small) signs of good faith on pursuing and prosecuting cybercriminals. No side will want to throw away what the two achieved in 2021.
- Standards: IoT's weaknesses will be addressed, in part, by a push for new security standards.

B. Human rights

- Ethics: AI has had its fair share of attention; metaverse is next. Expect deeper reflections on technological progress and humanity's future, and on a new (digital) social contract.
- GDPR: Data transfers of European citizens to the USA need a legal basis. Companies will call for legal certainty and for rapid outcomes to ongoing negotiations.
- Inequalities: As the pandemic starts to lose its grip, we'll be coming to terms with the digital gaps it exposed and exacerbated.

C. Social and economic development

- Antitrust (and gig work): Expect new antitrust rules from the EU (DMA/DSA) and from China, and more legislative debates in the USA.
- WTO: If the group of like-minded countries working under the Joint Statement initiative are as successful as last year, it would mark a comeback for the WTO.
- Semiconductors: Expect new rules from the EU and major investment by US companies to wean off their dependency.

A month-by-month forecast: Top events to follow in 2022

The digital policy calendar in 2022 will be as busy as ever. Not only will it include the events on typical issue areas of digital policy (cybersecurity, e-commerce, and the rest), but will also feature mainstream events which will tackle digital aspects. Here's our list of events to watch for.

FEBRUARY

The fourth [Global Standards Symposium](#), taking place in Geneva, Switzerland. The theme of GSS-20 is 'International standards to enable the digital transformation and achieve the sustainable development goals (SDGs)'. GSS-20 will conclude with an outcome document to be presented at WTSA-20. Also scheduled for February is a [one-day meeting of the UNODC's Ad Hoc Committee](#) – the body tasked with negotiating a cybersecurity convention – which will look into organisational matters. The [UN Human Rights Council's 49th session](#) also kickstarts this month.

MARCH

Held every four years, the World Telecommunication Standardization Assembly (WTSA) defines the next period of study for the ITU's Telecommunication Standardization Sector (ITU-T). [WTSA-20](#) will take place in Geneva from 1–9 March 2022. The [World Summit on the Information Society \(WSIS\) Forum 2022](#), co-organised by ITU, UNESCO, the UNDP, and UNCTAD, kickstarts in mid-March with the theme 'ICTs for Well-Being, Inclusion, and Resilience: WSIS Cooperation for Accelerating Progress on the SDGs'. The second session of the [Open-ended Working Group \(OEWG\)](#) on cybersecurity will take place at the end of the month.

APRIL

UNCTAD's [eCommerce Week 2022](#) will be dedicated to data and digitalisation for development. There's a special focus on data and cross-border flows and the critical role they play in economic and social development, as well as challenges related to the data divide. Plus, discussions will take place on how the COVID-19 pandemic is affecting digital transformation globally.

MAY

The [7th Multistakeholder Forum on Science, Technology, and Innovation for the Sustainable Development Goals \(STI Forum\)](#), whose theme reflects that of July's High-Level Political Forum, will look at a post-pandemic world through the lens of science, technology, and innovation. Also scheduled for May is [RIPE84](#), a regular meeting of the regional internet registry for Europe, where ISPs and network operators will tackle technical issues such as the deployment of IPv6, the IoT, and connectivity.

JUNE

Organised by ITU, this year's [World Telecommunication Development Conference](#) (WTDC-21) in Ethiopia will focus on how to expand internet access to achieve the SDGs (and on the selection of ITU's next head). Towards the end of the month, it will be Germany's turn to organise the [G7 Summit](#) as holder of this year's presidency. The [top priorities for Germany](#) are climate change and economic recovery, as well as strengthening global health, pushing for sustainable development, and advancing human rights, and digital inclusiveness. There's also the UN Human Rights Council's 50th session this month.

JULY

At the [High-level Political Forum \(HLPF\)](#) on Sustainable Development, from 5–7 and 11–15 July, it's the turn of SDGs 4 (quality education), 5 (gender equality), 14 (life below water), 15 (life on land), and 17 (partnerships) to be reviewed. The forum will also take a deeper look into the impact of the pandemic across all SDGs. The dates include a three-day ministerial segment.



AUGUST

Tentatively scheduled for August is the [African Peering and Interconnection Forum \(AfPIF\) 2022](#), to be hosted by the Rwanda Internet Community and Technology Alliance (RICTA). The forum will address the key interconnection, peering, and traffic exchange opportunities and challenges in Africa.

SEPTEMBER

In mid-September, keep an eye on the [77th session of the UN General Assembly \(UNGA\)](#) (where world leaders will announce their priorities and concerns for the coming year), the [World Trade Organisation \(WTO\)'s 2022 Public Forum](#), the [Shanghai Cooperation Organisation Summit](#), and the UN Human Rights Council's 51st session. Towards the end of the month and sliding into October, the [ITU Plenipotentiary Conference \(PP-22\)](#) will see countries gather in Bucharest, Romania. Among other agenda items, countries will vote for a new ITU leadership.

OCTOBER

There's a second RIPE meeting this year: it's the 85th meeting, taking place on 24–28 October. The [14th BRICS Summit](#), hosted in China, is likely to be scheduled for October if it follows last year's schedule.

NOVEMBER

The [G20 Leaders' Summit](#) will take place 15–16 November in Bali. Indonesia's presidency will focus on global health architecture, sustainable energy transition, and digital transformation. The annual [Internet Governance Forum \(IGF\)](#), hosted by Ethiopia, is scheduled for the second half of the month, as well as the 4th [Paris Peace Forum](#), which showcases projects that tackle pressing global issues.

DECEMBER

Organised by the IEEE, the [2022 edition of the Global Communications Conference \(GLOBECOM\)](#) will focus on digital transformation through smart communications. Expect a programme that includes symposia, tutorials and workshops, keynotes and panels, business and industry panels, and vendor exhibits.

Digital policy developments that made headlines in January

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



Same relevance

Global architecture

UN Secretary-General Antonio Guterres [urged member states](#) to 'speed up work on banning lethal autonomous weapons, and to begin considering new governance frameworks for biotechnology and neurotechnology'.

Australia and the UK [concluded a new Cyber and Critical Technology Partnership](#).



Decreasing relevance

Sustainable development

China published a [plan to foster the development of the country's digital economy](#). [Malaysia launched two initiatives](#) to support digital trade and the growth of the digital economy.



Increasing relevance

Security

Ukraine [accused Russian hackers of being behind a massive cyberattack](#), taking down about 70 government websites. [Russia took down](#) ransomware crime group REvil.

A [cyberattack targeted personal data held by the International Committee of the Red Cross \(ICRC\) on over 500,000 vulnerable people](#).

Experts and civil society groups urged the Ad Hoc Committee working on a potential UN cybercrime treaty [to embed human rights protections](#) in the document.

The UK announced [draft legislation to improve cyber resilience](#).

Figures released by the Internet Watch Foundation show that [2021 was the worst year for child sexual abuse online](#).



Increasing relevance

E-commerce and the internet economy

[France's data protection authority fined Facebook and Google](#) for not complying with cookie rules. [China's market regulator fined tech companies](#) for undeclared acquisitions. The [US Federal Trade Commission \(FTC\) and the US Department of Justice announced a review of merger and acquisition approvals](#) to 'address unique problems raised by the tech industry'.

The [European Parliament adopted the Digital Services Act](#), paving the way for further negotiations on the act, between the Parliament, Commission, and Council. *More on pages 8–9.*

[Indonesia banned financial institutions](#) from using, marketing, or facilitating crypto asset trading. Diem Association – a Facebook-backed crypto initiative – [announced the sale of its assets](#).



Same relevance

Infrastructure

The European Commission launched a [tender for the deployment of a recursive European domain name system \(DNS\) resolver service infrastructure](#).

The Wi-Fi Alliance [announced a new wireless standard](#). The Coalition for Content Provenance and Authenticity [launched a technical specification for content provenance](#).

Digital rights

The European Commission proposed a [European declaration on Digital Rights and Principles](#).

[Meta was sued in the UK for gathering users' data](#) without compensating them. The [European Commission asked WhatsApp to clarify its personal data processing practices](#) by the end of February.

The [European Data Protection Supervisor ordered Europol to erase personal data](#) not related to crime.

Civil society groups called on the UAE to [bring its new law on combating rumours and cybercrime in line with international human rights standards](#).

Internet access disruptions were recorded in [Kazakhstan](#), [Yemen](#), and [Burkina Faso](#).

Content policy

The US Congress committee investigating the 2021 Capitol attack [ordered YouTube, Facebook, Twitter, and Reddit to provide records](#) relating to the spread of misinformation and violent extremism.

In France, [Twitter lost an appeal](#) against a court order asking the company to disclose details of actions against hate speech. Nigeria [lifted its ban on Twitter](#).

Jurisdiction and legal issues

The Austrian Data Protection Authority [ruled that Google Analytics](#) (in German) violated the EU's General Data Protection Regulation.

In the USA, four attorneys general [sued Google over use of 'dark patterns' to track people's location](#). The General Court of the EU [annulled a €1.06 billion fine imposed on Intel by the European Commission](#) in 2009.

New technologies

China issued [new rules for algorithm recommendation technologies](#) (in Chinese) and published a [draft regulation for deepfake technologies](#) (in Chinese). The UK announced the [establishment of an AI Standards Hub](#).

Egypt's telecom regulator issued a [regulatory framework for providing IoT services](#).

[France launched a quantum computing platform](#) to facilitate access to quantum resources for researchers and companies.



Increased relevance



Decreasing relevance



Increased relevance



Increased relevance

DSA and DMA: A start-of-year recap

This will be a critical year for the regulation of tech companies. Europe is progressing particularly fast: The draft Digital Services Act and a Digital Markets Act are now being negotiated by the European Parliament and the EU's Council (representing member states). Here, we track their progress and what this means for Big Tech.

Transatlantic affairs

There's a lot going on right now in transatlantic digital affairs. The USA and the EU are working out a new post-Privacy Shield arrangement (that will give US companies the legal basis they need for transferring EU citizens' personal data to the USA). There are also home turf negotiations on how to implement the OECD's new global tax deal. Over at the Trade and Tech Council, how to cooperate on semiconductors is one of the main issues.

In addition, there will soon be two new pieces of EU legislation – the Digital Services Act (DSA), and the Digital Markets Act (DMA) – that will impact Big Tech directly. The pressure is on for policymakers, as the French Presidency of the EU Council wants to see these materialised as soon as possible.

Regulating tech companies

Both draft laws aim to regulate online platforms, which is why they are often discussed together. Yet, they regulate different aspects.

The DSA is concerned with harmful and illegal goods, services, and content online. The DMA addresses competition and antitrust issues. *See the fact box on the next page.*

Don't discriminate

Across the pond, the US government is in a bit of a bind. It wants to advance its antitrust agenda on its home turf, but also wants to defend US tech firms overseas. Of the two, the transatlantic issue is a more serious problem. It's [been reported](#) that the US government has called on EU policymakers not to raise the threshold for defining gatekeepers under the DMA. The higher the thresholds, the more concentration around Big Tech the law will be – something the USA thinks is discriminatory.



There's even more bipartisan pressure on the administration to tackle this with the EU. The [Senate Finance Committee thinks](#) that both laws 'must apply equally to firms based in Europe, China, the United States, and other countries' in order to not give non-US companies a competitive advantage. Still, this argument is unlikely to hold water, considering that the world's most valuable tech companies [are US companies](#).

Back to our first prediction

Perhaps the biggest worry, at least for Europe's network of consumer organisations, is that Big Tech companies are able to dilute the rules during the triologue phase. 'Big Tech firms are therefore throwing immense resources (that they can easily afford) on a scale rarely seen to influence, persuade and cajole members of the European Parliament, member state governments and European Commission officials to roll back the obligations the DMA would impose', [BEUC's deputy director-general wrote](#).

'Not only are they lobbying in their own names, but they are also deploying trade associations, think tanks and "favourable" academics to mirror, endorse, and amplify their arguments. They have even claimed to represent the best interests of small and medium-sized companies (!), much to the annoyance of genuine SME representatives.'

Talk about a tug-of-war.

FACTBOX	The Digital Services Act (DSA)	The Digital Markets Act (DMA)
<p>What will they regulate?</p>	<p>They both aim to regulate tech companies:</p>	
	<p>The DSA is concerned with harmful and illegal goods, services, and content online.</p> <p>It will replace the E-Commerce Directive (2000).</p>	<p>The DMA is concerned with competition and antitrust issues.</p> <p>It will broaden the range of existing measures for investigating and correcting market practices by creating ex ante rules that prohibit certain behaviours.</p>
<p>Who will be regulated by the new laws?</p>	<p>Intermediary services, that is, companies whose business places them between sellers and customers.</p> <p>Companies will be categorised according to the type of service they offer, that is:</p> <ul style="list-style-type: none"> ● Basic intermediary service providers, including ISPs, domain name registrars, etc ● Hosting service providers, including cloud, web hosting services, etc ● Online platforms, including marketplaces and social networks ● Very large online platforms, that is, those with at least 45 million average monthly active users. <p>These definitions are still up for debate. The EU Council, for instance, thinks that the law should include a reference to online search engines; there's no such reference in the Parliament's draft.</p>	<p>Gatekeepers, which in practice means only a small number of tech companies.</p> <p>The original proposal defines gatekeepers as those companies that control core services on the internet, and which service more than 45 million users and 10 000 business users in the EU per month.</p> <p>One open issue relates to this definition. The European Parliament, for instance, thinks that smart devices such as virtual assistants should be added to the list of core services due to their growing demand. The Council calls this 'voice assistant technology', which could be interpreted a bit differently.</p> <p>Another question relates to the size of companies: the proposal targets companies with more than €8 billion in annual turnover and a market value of €80 billion. While the Council and Parliament are likely to agree, there will be rebukes from across the ocean.</p>
<p>How will they be regulated?</p>	<p>This depends on the type of intermediary services. The original proposal describes a basic set of obligations for intermediary service providers but heftier rules for the other categories. This means more transparency and consumer protection-related obligations for these companies.</p> <p>Up for serious debate is a list of stricter obligations for online marketplaces and very large online platforms – such as rules on how to tackle illegal and harmful content – something which both the Council and the Parliament want. This is where the crux of DSA negotiations lies.</p>	<p>The original proposal lists what a gatekeeper is prohibited from doing, such as giving preference to its own goods and services over those of others using its platforms.</p> <p>Things a gatekeeper should do include allowing users to uninstall native software and allowing business users access to the platform's data.</p> <p>The Council and Parliament are asking for more. For instance, a ban on the use of children's data and easier ways for users to unsubscribe from a core service. The devil will be in the details.</p>

How will digital standards shape geopolitics?

After a lot of positioning last year, digital standards will this year regain a central focus in geopolitics. This text provides a short 'navigation guide' for the digital standardisation space.

Why?

Standards provide blueprints for future tech developments – from data flows and AI, to 6G and consumer economics. By influencing digital standards, companies and countries will try to promote their values, interests, and technical strengths. Digital standards, especially in AI and data, will have far-reaching consequences on human rights as well.

When?

There are two 'temporal' aspects of digital standardisation. First is historical evolution consisting of three main phases in digital standardisation: during the 1980s, the dominant actors were the USA, the UK and Germany; during the 1990s the shift towards Asia started with the prominent roles of Japan and South Korea reflecting their fast digitalisation; during the 2010s China emerged as a prominent actor especially concerning Huawei's impact on 5G standards. China's growing standardisation footprint has prompted increasing interest in digital standards in the media and governments worldwide.

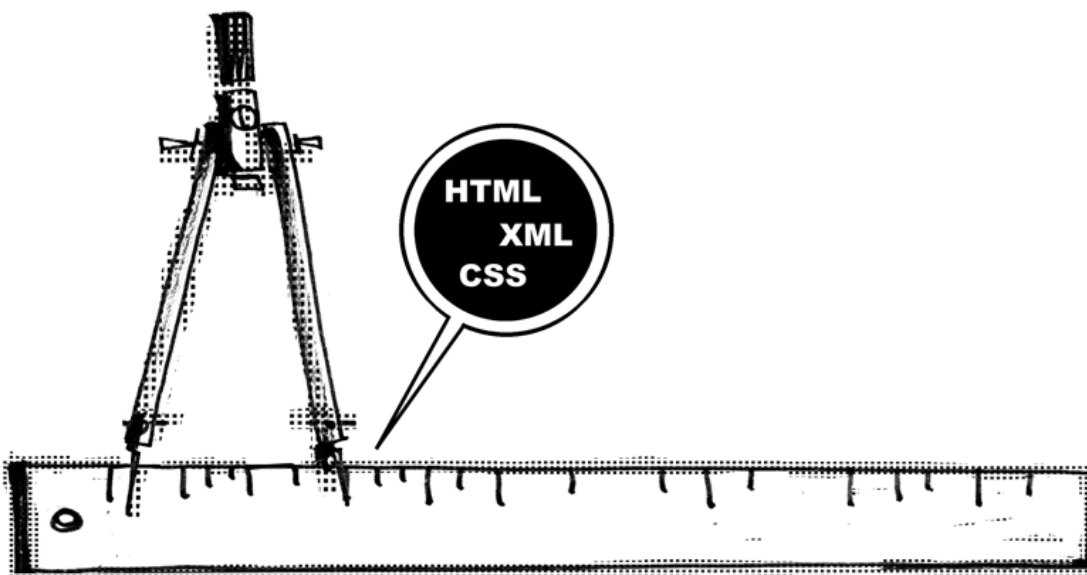
The second temporal aspect is the duration of the standardisation process ranging from the extremely short duration of 9 months, which rarely happens to 18 months, which is realistic and fast to 3-4 years which is the most common duration needed to develop digital standards.

Who?

Two leading tech powers – the USA and China – are positioning themselves as the major actors in digital standardisation. The USA's tech experts and companies have been shaping digital standards for decades, including core internet norms and telecommunications standards.

During the 2010s China ramped up its efforts at being active in as many forums as possible. It is part of the broad Chinese strategy to evolve from being a user to a producer of digital standards. For example, its go global approach, China tries to export national automobile standards for self-driving and autonomous vehicles on a global level.

Standards play a critical part in the EU's value-based digital policy as a way to link technology to human rights, the rule of law, and



global public goods. India and other actors, mainly from Asia, are increasing their involvement in digital policy. Most African and developing countries are absent from digital standardisation processes.

Standardisation organisations in Geneva work on more inclusive standard-making processes via capacity building, peer learning, seminars, and publications as outlined in, for example, ISO's [action plan](#).

What?

Thousands of standards shape our digital world, from the way hardware is designed to how internet traffic flows. However, some standards are more prominent in public discourse.

The New Internet Protocol (IP) caused considerable stir in 2019 when it was proposed in ITU-T's Telecommunication Standardization Advisory Group (TSAG) by Huawei, China Mobile, China Unicom, and MIIT.

The New IP was presented as a way to design 'a new information and communications network with [a] new protocol system that satisfies and serves for the future.'

The concerns were diverse – from those that suggested that users' privacy would be affected to arguments that it would replicate something which already existed and worked well. Eventually, the proposal was shelved, but there are several lessons to be learned from this process.

AI, data flows, facial recognition, quantum computing, IOT, and 6G are among the issues that will emerge on the standardisation agenda.

Where?

Traditionally, digital standards have been developed by international standardisation organisations (ISOs) based in Geneva: the International Standardisation Organisation, the International Telecommunication Union, and the International Electrical Commission.

Second, a wide range of highly influential technical and business standardisation organisations and initiatives are involved, including the IETF for the internet, the 3GPP for 5G, and IEEE for AI.

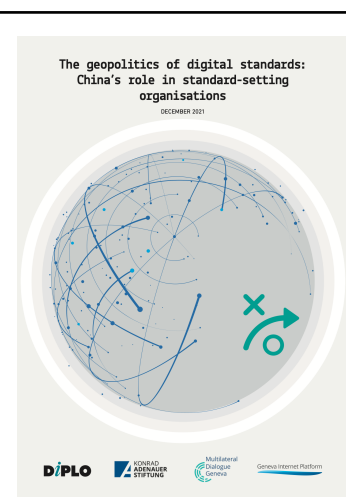
Digital standards have also been raised in diplomatic agendas worldwide. For example, China is pursuing digital standards in APEC, BRICS, and the Belt and Road Initiative. Digital standards are high on the agenda of the [US-EU Trade and Technological Commission](#).

How?

Digital standardisation processes will be shaped by the interplay between strategic competition and the necessity for cooperation. There is a shared and strong interest of tech companies from both China and USA to have common digital standards globally enabling easier access to markets worldwide.

On the modus operandi of digital standardisation, the main challenge has been to build cross-cutting impacts of digitalisation into new standards by design. For example, technical standards for facial recognition directly impact privacy protection. AI standards can support the right to non-discrimination. Environment and digital will come into closer proximity through standards for dealing with e-waste and the circular economy.

For in-depth information, consult [The geopolitics of digital standards: China's role in standard-setting organisations](#), a study published by Diplo/Geneva Internet Platform and Multilateral Dialogue Konrad Adenauer Foundation Geneva. Consult also the [digital standards section](#) of 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.

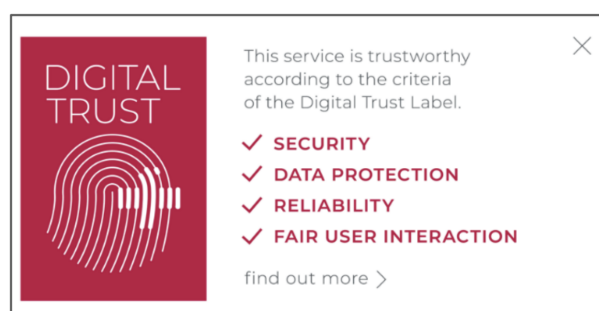
18 January | Swiss Digital Initiative's launch of the Digital Trust Label

After more than two years in the making, the [Swiss Digital Initiative launched the Digital Trust Label](#), which marks the world's first label for digital responsibility.

SDI Foundation president Doris Leuthard explained: 'Similar to the organic label and a nutrition facts table, the Digital Trust Label acts as a seal of trust in the digital world.'

In order to obtain the label, digital services are audited on 35 criteria related to security, data protection, reliability, and fair interaction with the users. The criteria catalogue was created by the Label Expert Committee, under the

leadership of École polytechnique fédérale de Lausanne (EPFL), and chaired by Stephanie Borg Psaila, Diplo's Director for Digital Policy (and editor of this newsletter).



25 January | Roundtable – How to prevent cyber threats and participate in cyber peace

The [roundtable, organised by the CyberPeace Institute](#), addressed the rise of cybercrime and cyberattacks and the most widespread cyber threats. Panellists from the private sector and

international organisations discussed solutions and practices that can be adopted to prevent and mitigate the issues and to work collectively towards a more peaceful cyberspace.

25-27 January | DC³ Conference – From Cryptocurrencies to CBDCs

The [three-day Digital Currency Conference \(DC³\)](#) organised by the Digital Currency Global Initiative, a joint collaboration between ITU and the Future of Digital Currency Initiative at Stanford University, brought together industry experts and practitioners to discuss the latest developments related to central bank digital

currencies (CBDCs), cryptocurrencies, and stablecoins. The parallel tracks and deep-dive sessions looked at standardisation issues and cross-border interoperability, security and privacy challenges, and financial inclusion. If you missed the event, recordings of the sessions and presentations [are available](#).

About this issue: Issue 66 of the Digital Watch newsletter, published on 7 February 2022 by the [Geneva Internet Platform](#) and [DiploFoundation](#), under a [CC BY-NC-ND 4.0 licence](#) | Contributors: Stephanie Borg Psaila (editor), Andrijana Gavrilovic, Kristina Hojstricova, Jovan Kurbalija, Dorijan Nadjovski, Virginia (Ginger) Paque, Sorina Teleanu | Editing and design: Aleksandar Nedeljkov, Viktor Mijatović, and Mina Mudrić | On the cover: Predicting 2022. Credit: Vladimir Veljašević | Feedback? [Drop us a line](#).

The Geneva Internet Platform is an initiative of:

