GENEVA INTERNET PLATFORM
digwatch

NEWSLETTER

Issue 58 – Wednesday, 7th April 2021

Fit for travel

BAROMETER

Things are stirring on the global policy architecture, content policy, internet economy, and security fronts.

Pages 4–5

BIG TECH vs BIG TECH

Friends-turned-foes are making their feelings known. And they're not pleasant.

Page 6-7

FACIAL RECOGNITION

The case of Clearview AI has heightened government interest to regulate the technology.

Page 8-9

OEWG DIPLOMACY

After months of work, the cyber group adopted its final report. In our legal section, we take a look at the report...

Page 10

The top digital policy trends in March

Each month we analyse hundreds of unfolding developments to identify key trends in digital policy and their underlying issues. Here's what mattered in March.

Fit for travel

It's been a year since the World Health Organization (WHO) declared the COVID-19 virus a global pandemic. Throughout this time, technology's role in the service of medicine – in identifying the virus, curbing its spread, and developing vaccines – has been nothing short of extraordinary.

Now that vaccination efforts are underway in most countries, there's hope that we'll soon be able to move around and travel more easily. Fuelling this hope is technology's latest product: digital vaccine passports (for an overview, read last month's article).

In some countries, good ol' paper-based vaccination certificates are already being complemented by their digital equivalent, which takes the form of a QR-code on a traveller's mobile device that can be verified much faster at control points. Some countries, such as Israel, Australia, Greece, and Estonia, are way ahead in rolling out digital certificates. Others, including the EU, are trailing behind. The USA is also mulling the idea, albeit at a more reserved pace.

If digital vaccine passports (also known as green passes) are also used to ease physical distancing rules that are preventing unrestricted entry into shops, entertainment venues, and offices, they could be pivotal in resetting the economy.

Governments will need to tread with caution, though. If vaccines are already giving a false sense of security to those who think they are 100% effective, vaccine passports will stretch this false idea further.

More importantly, in order for digital vaccine passports to prove their worth, their framework – built upon interoperable standards and strong data protection safeguards for the sensitive medical information they carry – needs to be developed fast. For now, it's mostly 'papers, please'.

The good ol' paper-based certificates will have a digital equivalent. Credit: European Commission

Cyber diplomacy in action

If the work of the 2015 UN GGE group ended on an uneventful note for cyber diplomacy, that of the Open-ended Working Group (OEWG) – which a fortnight ago reached consensus on its final report – reignited the embers.

Touted as a landmark document for cybersecurity and international relations, the final report reaffirms what was agreed to in previous documents. Although it may sound like a futile exercise to revisit past work, this agreement serves to cement the status of previous final reports as a collective *acquis* (*more on page 6*), and represents a moment where UN member states have finally reached consensus in an area typically full of hostility.

Cyber diplomacy has been in action in other quarters too. Australia, India, Japan, and the USA (known as the Quad) agreed to create a working group for critical and emerging tech. The OSCE Informal Working Group resumed its work on how to operationalise confidence-building measures (CBMs), which are meant to reassure countries concerned with another country's intentions in the domain of cybersecurity and cyberwarfare. These developments bode well for multilateral relations at a time when the world needs countries to row in the same direction.

On the path to 'becoming'

From time to time in the geopolitical world, country- or region-wide strategies remind us of their ambitious plans for tech leadership. For both the EU and China, which revealed new plans in March, leadership also means being more technologically self-reliant.

The EU's Digital Compass sets new targets linked to skills, infrastructure, and digitalisation of businesses and public services. The EU will take any member country's lagging progress seriously. Its plan includes a monitoring system with annual reporting in the form of 'traffic lights', to help make sure EU countries stay on track.

China's new five-year plan carries a strong focus on technology, with new ambitions in cutting-edge tech including new-generation AI and quantum information. Once again, the country strongly reiterates the need for becoming self-sufficient, alluding mostly to its reliance on the USA for semiconductors.

As the ongoing trade war between China and the USA has shown, however, these ambitions will not be easily and quickly achieved. It will take time – and significant investment – for scientists and engineers, and especially the next generations, to pump expertise into home-grown industries. Judging by the huge investments outlined in its plan, China is poised to continue inching ahead.

In case you missed it...

The UK's Royal Navy will build a surveillance ship, fitted with advanced sensors and autonomous undersea drones, to protect undersea cables. Defence Secretary Ben Wallace warned 'the lights could go out' if national infrastructure was lost, and the UK would be 'deeply exposed' without further measures.

Credit: PA Media

Digital policy developments in March

The digital policy landscape changes on a daily basis. Our aim is to decode, contextualise, and analyse ongoing developments, offering a digestible yet authoritative update. There's more detail in each update on the *GIP Digital Watch* observatory.


increasing relevance

Global IG architecture

Australia, India, Japan, and the USA (the Quad) created a critical and emerging technology working group. Over 20 companies called on the G7 to establish a Data and Technology Forum.

Stakeholders have different views on whether and how a multistakeholder high-level body (envisioned in the Roadmap for Digital Cooperation) should be created within the IGF.


same relevance

Sustainable development

The African Development Bank allocated US$2 million to strengthen cybersecurity and financial inclusion in Africa and US$2.33 million to support Ethiopia's modernisation of its e-payments infrastructure.

The UK launched a £2.5 million fund to improve digital inclusion for people with learning disabilities. Malawi's new Digital Economy Strategy aims at expanding access to affordable internet. Sri Lanka announced its first financial inclusion strategy.


increasing relevance

Security

The OEWG adopted its final report.

Microsoft disclosed that vulnerabilities in its Exchange server have been exploited since January 2021 by 'actors assessed to be state-sponsored and operating out of China'.

Belgian, French, and Dutch police forces took down the encrypted messaging platform SKyECC used by large-scale organised crime groups.

Norwegian and German parliaments suffered cyberattacks.

The UN Committee on the Rights of the Child adopted General Comment 25 on children's rights in the digital environment.


increasing relevance

E-commerce and the internet economy

China fined 12 internet companies for breaking anti-monopoly laws.

Four US states joined the antitrust lawsuit launched against Google in December 2020. The UK competition regulator opened an investigation into Apple over its App Store practices, and found that Facebook's purchase of Giphy raises competition concerns.

Epic Games sued Google in Australia for allegedly restricting competition in payment processing and app distribution. It also filed a complaint against Apple in the UK over similar issues.

The European Commission reiterated plans to present a proposal for a digital tax by June.

Uber announced it will comply with a recent court decision to grant UK drivers minimum wage, holiday pay, and pensions.


same relevance

Infrastructure

The European Commission announced new digitalisation targets under the 2030 Digital Compass. A coalition of internet companies asked the US Federal Communications Commission (FCC) to reinstate net neutrality.

The US administration placed new restrictions on companies that supply equipment to Huawei. Facebook announced plans to build two subsea cables to connect Singapore, Indonesia, and North America.

Digital rights


same relevance

The USA and the European Commission announced an intensification of negotiations on an enhanced Privacy Shield Framework. A federal data protection bill was introduced in the US Congress.

The French data protection authority (DPA) opened a privacy investigation into the social media app Clubhouse.

The Indian government asked the Delhi High Court to block the implementation of WhatsApp's new privacy policy.

Facebook published its first human rights policy.

Swiss citizens voted against an electronic identity system.

Internet services were disrupted in Senegal and Myanmar amid political unrest.

Content policy


increasing relevance

Russia threatened to block Twitter if the platform does not remove banned content. China reprimanded LinkedIn for failing to monitor objectionable political content.

The Council of the EU adopted a regulation requiring platforms to remove or disable access to terrorist content within one hour of notification.

The UN Special Rapporteur on Minority Issues called for an international treaty to address hate speech against minorities.

Reporters Without Borders sued Facebook in France over the proliferation of hate speech and misinformation.

The CEOs of Alphabet, Facebook, and Twitter testified in the US Congress on the role of social media in spreading misinformation and fostering extremism.

Facebook ended the temporary ban on ads about social issues, elections, and politics in the USA.

Jurisdictional and legal issues


same relevance

US legislators re-introduced the Journalism Competition and Preservation Act to help small news organisations negotiate with tech platforms.

The Court of Justice of the European Union (CJEU) ruled that access to traffic or location data can be allowed only for investigating serious crimes and preventing serious threats to public security. In a different case, the court ruled that websites displaying links to copyrighted material under contract may be subject to restrictions imposed by the copyright owner.

New technologies (IoT, AI, etc.)


increasing relevance

China's new five-year plan highlights support for AI, quantum information, and other frontier technologies.

The US National Security Commission on Artificial Intelligence released its final report to the US Congress and the President.

The Committee of Ministers of the Council of Europe drew attention to the human rights implications of using AI-enabled decision-making in the area of social services.

The European Commission proposed a Green Digital Certificate to facilitate free movement within the EU during the COVID-19 pandemic.

Big Tech vs Big Tech

Big tech companies' once-united front has been damaged by public attacks against each other. The friends-turned-foes are making their sentiments known. What has triggered this change?

In July 2020, America's four largest tech companies – Google, Apple, Facebook, and Amazon, collectively known as GAFA – appeared together before the US Congress as part of an investigation into the dominance of tech companies. As we wrote back then, the CEOs had differing, but ultimately shared opinions. Their written statements were strikingly similar, showing a united front.

Since then, the relations between tech companies have been gradually turning sour. When Apple announced that it would introduce a new feature to its iOS requiring users to give apps permission to track them, Facebook made its complaints public with full-page adverts in *The Wall Street Journal*, *The New York Times*, and *The Washington Post*. Apple's Tim Cook responded with a tweet.

In January, Facebook escalated its public grievances during its quarterly earnings call: 'We have a lot of competitors who make claims about privacy that are often misleading.' Hitting back, Apple CEO Tim Cook criticised the digital ad business model during the CPDP 2021 data protection annual conference: 'Technology does not need vast troves of personal data, stitched together across dozens of websites and apps, in order to succeed.'

In March, it was Google and Microsoft's turn to trade punches. At a hearing of the US House Judiciary subcommittee on antitrust, Microsoft President Brad Smith told lawmakers that journalistic outlets have been forced to 'use Google's tools, operate on Google's ad exchanges, contribute data to Google's operations, and pay Google money.' In a blog post, Google levelled its own criticisms at Microsoft, accusing the company of trying to divert attention away from two major hacking campaigns in which the software company was directly involved.

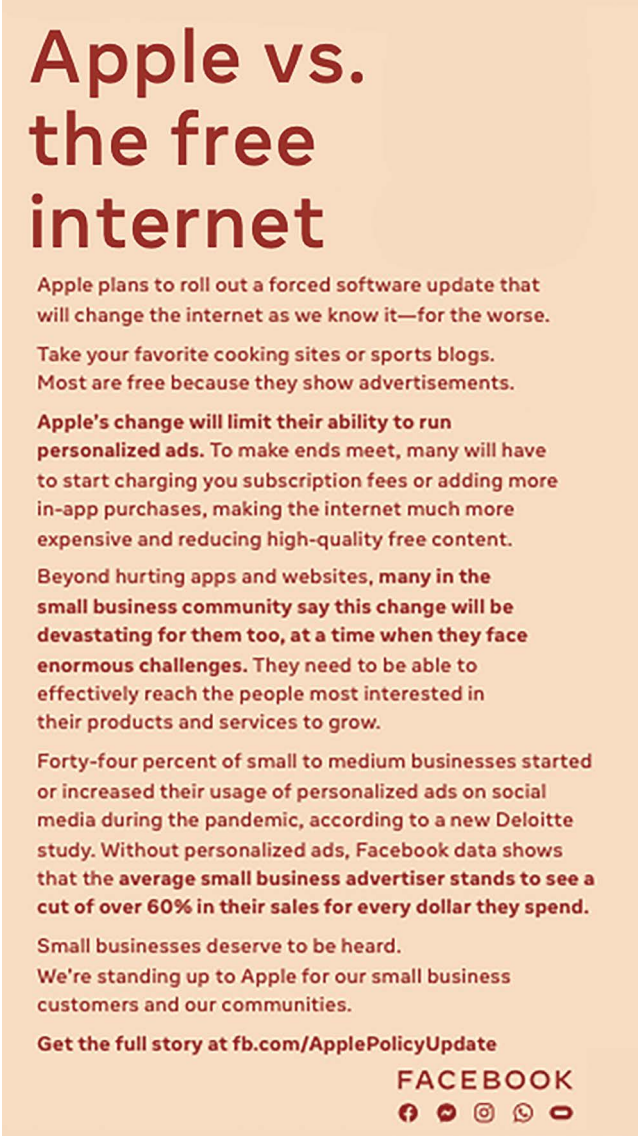
Friends-turned-foes

In the past decade, big tech companies in the USA have enjoyed market power in their respective domains: Facebook in the market for social networking, Google in online search and search advertising, Amazon in the online retail market, and Apple in the mobile operating system market. Although Microsoft is not a target in the ongoing antitrust efforts in the USA, its revenues place it solidly in the upper echelons of Big Tech.

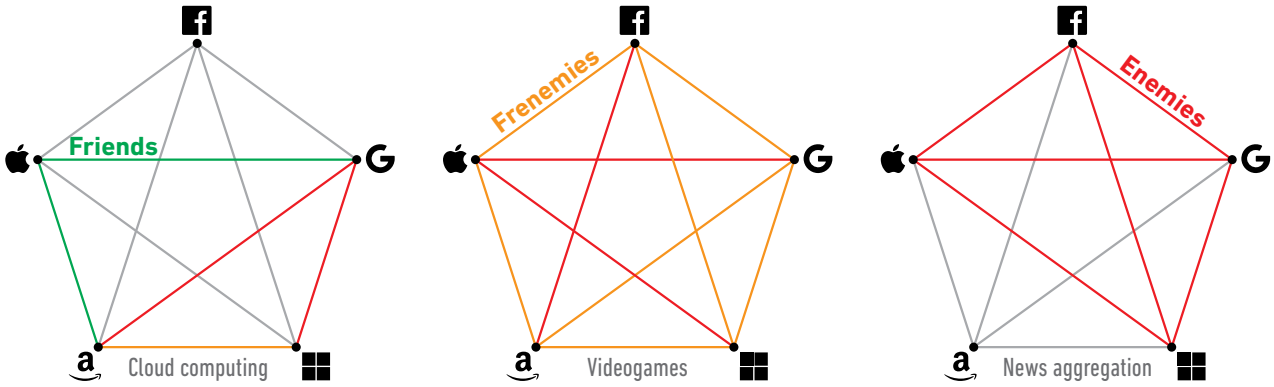
Their solid status in each of these domains was a good enough reason not to step on each other's toes. Sun Tzu's military advice – in 'attacking walled cities, one's strength is diminished' – is conventional Big Tech wisdom. But there are now at least three broad reasons for the shifting sands.

Monopolies are challenging each other

Diversification opens the door for growth and higher profitability. A few years ago, tech companies started broadening their reach to offline markets, venturing into postal services, grocery chains, and renewable



Facebook made its complaints public with full-page adverts. Source: Axios.com



Friends, Frenemies, Enemies. Credit: The Wall Street Journal (2021)

energy. Recently, their diversification efforts have led them to explore each other's markets.

As *The Economist* explained recently, the share of the five American giants' revenues is now overlapping with the others. Since 2015, the overlap has increased from 22% to 38%. The fiercest competition is happening in the cloud, with Microsoft and Alphabet taking on Amazon. In turn, Amazon is 'the rising force in digital advertising'.

The result is that monopolies are turning into an 'oligopoly of rivals'. This is resulting in direct competition. It's as if the monopolies' tacit pact has been broken.

Runners-up are winning

Smaller companies – and not just second and third runners-up – are breaking ranks. The pandemic has definitely helped.

A classic example is Zoom, a remote meeting software which was relatively unknown until last year. The company became a household name almost overnight. It saw its revenues increase by 326% in 2020, and is set to make similar profits this year. Although many people use more than one platform, Zoom's profits are Microsoft Team's losses (and vice-versa).

It's a similar landscape for ride-hailing-turned-food-delivery companies, and for smaller businesses which managed to beat larger incumbents at e-commerce with out-of-the-box technological solutions. Just like Zoom, their potential is huge; and just like Big Tech, their winning mantra is tech-driven diversification.

Tech's new policies are hurting them

Money aside, the failure to protect users' data has often laid bare the frailty of reputation. Not that this had any lasting impact on Facebook's bottom-line when the Cambridge Analytica scandal broke out, or Microsoft (and countless other companies) with every reported data breach.

Yet, companies have taken bold steps to improve some of their data protection practices. Among the most notable is Apple's decision to require users to give apps permission before tracking them (App Tracking Transparency in iOS 14).

Facebook will be negatively impacted by this change. Since this new tech policy will reduce the flow of targeted data from users' iPhones that refuse permission, Facebook will be unable to target ads – and generate the same revenues from its ad business – in the way it has been doing until now.

Microsoft, which was effectively knocked out of the search engine competition and instant messaging competition years ago, felt similarly aggrieved by Facebook and Google's [revenue] stand-off, defending Australia's new media bargaining code and WhatsApp's policy update, and was quick to promote the use of Bing and Skype.

Although all these developments do not hurt Microsoft directly, the company's arguments echo the sentiments of other actors impacted by these policies. Smaller media houses will remain affected by Facebook and Google's negotiating power, online marketing agencies will by Google's new third-party cookie policy, and app developers by Apple's iOS 14 update.

Antitrusters believe Big Tech is projecting an image of 'battling for core territory' while ignoring that 'describing this as a fight risks overlooking the broader ways in which the firms mutually benefit from their collective dominance'. Yet, the changing landscape is nonetheless denting Big Tech's dominant position.

Lights, camera, detection!

In just 50 years, facial recognition technology (FRT) has moved from the realms of science fiction to tangible reality. For many, it has become a part of daily life... without much awareness of its widespread use.

In the mid-1960s early pioneers of FRT, with the support of US intelligence and military agencies, began using computers to recognise the human face.

Today, more advanced FRT is in widespread use, from the filters we use on Snapchat, to controls at the borders and in football stadiums. What once involved manual marking of key facial features now includes an abundance of datasets of faces thanks to deep neural networks used in the development of FRT.

The case of Clearview AI

In recent months, US-based Clearview AI, whose facial recognition software is used in 26 countries worldwide, fell under the scrutiny of authorities.

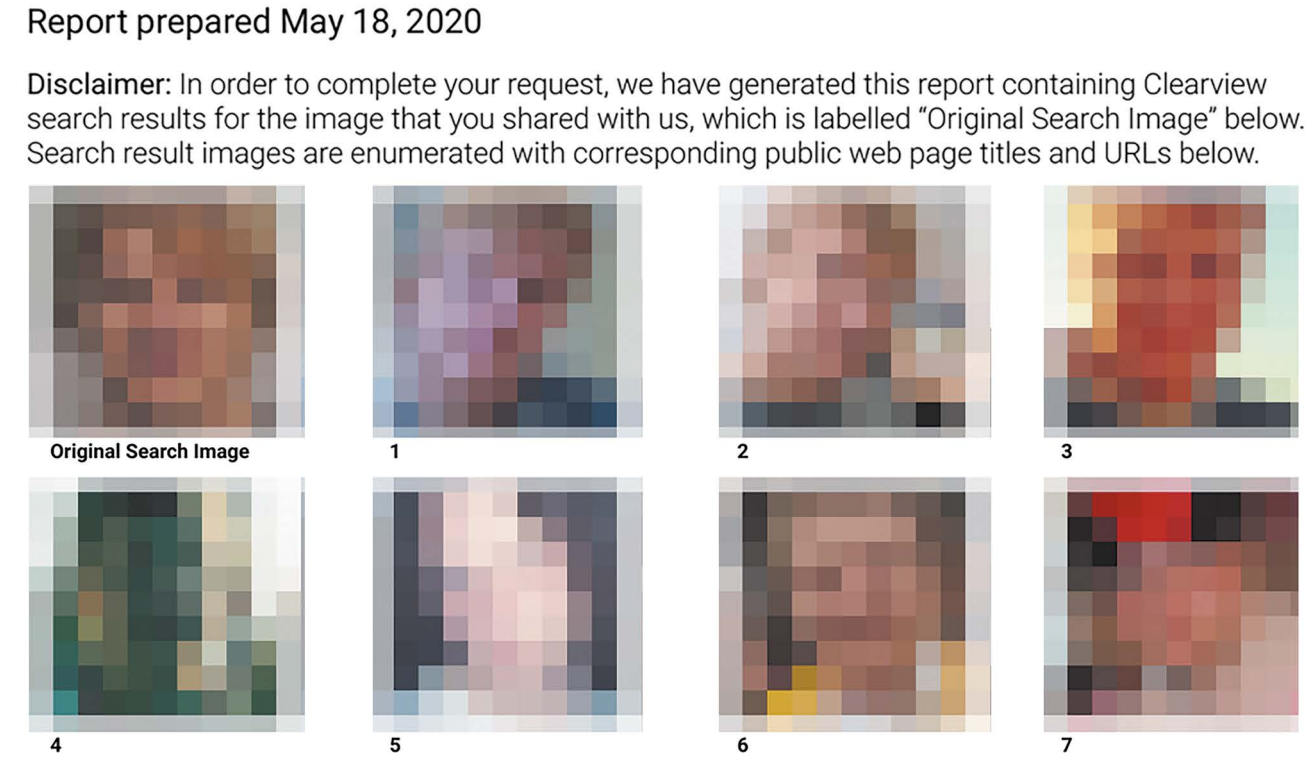
The company's software allows users to match pictures of people's faces to a database containing more than 3 billion images that have been scraped from social media platforms and other websites. The images are public, which means that the software works similarly to a search engine.

If that sounds simplistic, that's because it is. In the USA alone, more than 600 law enforcement agencies are using the software, with federal and state law enforcement officers declaring they have used its app to help solve shoplifting, identity theft, credit card fraud, murder, and child sexual exploitation cases.

Privacy experts, however, are not as keen on its use. They say the software scrapes data indiscriminately and raises concerns that the technology may lead us to a dystopian future. In California, the company was sued by two immigrants' rights groups over privacy rights violations, and in Canada, a joint investigation by four privacy commissioners concluded that the company violated the country's privacy laws by illegally obtaining photos and biometric facial arrays. The Swiss Federal Data Protection and Information Commissioner requested that the company destroy the data of Swiss citizens.

Mixed approaches to regulating FRT

Aside from Clearview AI's software, advances in facial recognition have sharpened governments' appetite to



A report generated by Clearview AI. Source: EDRI

Data analysis: FRT across the globe

FRT is used by public authorites in at least 113 countries. Our research shows that in most cases, it is used for crime prevention (39 countries), followed by border control (26 countries).

In most of the other use cases, the technology is part of a more generic smart city initiative, which includes the use of facial recognition for law enforcement purposes, and to access public services such as health and social security services. In a small number of countries, facial recognition is also employed in voting systems (Afghanistan, Paraguay, Sierra Leone, and Ghana).

COVID-19 and facial recognition

With the outbreak of the COVID-19 pandemic, a number of countries introduced contact tracing apps that use facial recognition. For example, France, Poland, El Salvador, and the Bahamas, to name a few, use the technology to impose social distancing measures, such as wearing masks and quarantine.

regulate the technology. So far, countries have taken a mixed approach.

Its use in public space has been banned outright in Belgium, Luxembourg, and Morocco, and in three US cities (Boston, Portland, and San Francisco). Other countries, including Spain, Denmark, and Sweden, have authorised the use of facial recognition systems to assist in crime prevention.

However, Europe is set to go further, and could set strong precedents like the GDPR did. precedents. In the EU, the European Parliament called for laws to regulate AI and facial recognition for military and non-military use, and asked the European Commission to consider a five-year moratorium on the use of digital facial recognition by public authorities and in public spaces.

The European Data Protection Board is similarly concerned: 'as it stands and without prejudice to any future or pending investigation, the lawfulness of such use by EU law enforcement authorities cannot be ascertained.'

The Council of Europe has also called for a ban on facial recognition unless appropriate rules are introduced.

Based on these cases, lawmakers around the world will need to decide on three issues: whether photos on social media platforms can be considered in the public domain; whether photos already made public require the user's consent to be used in an app like Clearview AI; and whether the use of software by law enforcement is in the public interest.

OEWG diplomacy: Zooming in on the final report

After months of work, the OEWG adopted its final report. This has cemented the status of agreed-upon reports as a collective acquis. We take a look at what's in the report.

The negotiations on the structure of such a report, the contents within each section, and the shifting of certain aspects to the chair's summary, show just how complex cyber diplomacy (the security side of 'cyber') is. Reaching consensus on a final report, for the first time in six years, was no minor feat.

In order to understand what the final report says, we need to keep in mind what the chair's summary signifies. These two documents are complementary: the final report contains what the states have agreed on; the chair's summary contains other issues for further discussion. The issues in the latter document did not make the cut for the report, but they remain on the record. One can argue that keeping institutional dialogue open is equally – if not more – important, than concluding ongoing debates. The chair's summary achieves precisely this aim.

What's included and what's not

The salient points included in each of the report's six sections – and the noticeable omissions – are:

- On existing and emerging threats: An acknowledgement of increasingly frequent and sophisticated harmful ICT incidents, and growing concern over attacks on a country's critical infrastructure, which undermines trust and confidence in political and electoral processes and public institutions. The report, though, fails to use more explicit language to describe threats arising from countries' misuse of each other's vulnerabilities.
- On norms, rules, and principles: Norms of responsible state behaviour are complementary to binding obligations under international law; among the norms is the need to ensure the availability and integrity of the internet.
- On international law: International law, and in particular the UN Charter, is applicable and essential to maintaining peace and stability. It falls short of making a specific reference to the applicability of the UN Charter 'in its entirety', and particularly that of international humanitarian law. Specifying this, some countries argued, would legitimise the militarisation of cyberspace. Only one principle of the UN Charter – the settlement of disputes by peaceful means – is referenced directly.
- On confidence-building measures (CBMs): The OEWG process itself was identified as a CBM, whose role is mainly to prevent conflict and share best practices.
- On capacity building: The report defines the principles, but misses out on an opportunity to mention existing international initiatives.
- On institutional dialogue: The final report recommends that dialogue continues at the UN, including the 2021–2025 OEWG and the so-called Programme of Action (a single, long-term, and inclusive process proposed by France and more than 40 other states). No mention is made of the need for inclusivity; neither is there any mention of the topics for discussion, leaving open the possibility of expanding the processes' mandate.

What's next?

The new OEWG starts its work soon with an organisational meeting on 1 June. Meanwhile, the work of the UN GGE is also about to end in May. We'll soon know whether it will signify another feather in cyber diplomacy's cap.

For more analysis, read A new landmark in global cybersecurity negotiations: UN Cyber OEWG in numbers (18 March 2021), and What's new with cybersecurity negotiations? UN Cyber OEWG Final Report analysis (19 March 2021), written by Geneva Internet Platform experts. Learn more about the OEWG and UN GGE processes in our dedicated space.

Amb. Jürg Lauber, chair of the OEWG

Policy discussions: Updates from Geneva

Many policy discussions take place in Geneva every month. The following updates are from March's events. For other event reports, visit the Past Events section on the *GIP Digital Watch* observatory.

Blockchain Technologies for Sustainable and Resilient Resilient Recovery from the COVID-19 Pandemic 15 March 2021

Organised by the Permanent Missions of Israel, Slovenia, and Switzerland to the UN Office in Geneva, the discussion looked at how blockchain technologies can help achieve the SDGs while ensuring a sustainable and resilient recovery from the COVID-19 pandemic. The debate, which focused on the UNECE Region, was organised on the sidelines of the UNECE Regional Forum on Sustainable Development.

Future Networked Car Symposium 22–25 March 2021

The symposium debated the policy and regulatory issues regarding automated vehicles, such as vehicle cybersecurity frameworks, vehicle communication, and current regulatory frameworks.

Data and Technology for Development | Road to Bern...via Geneva 25 March 2021

Organised by the Permanent Mission of Switzerland to the UN in Geneva and the GIP, the online dialogue tackled how to make sense of complex data sets and communicating findings in a simple way to better inform policy-making, as well as how technology applications can help the development agenda. Co-hosted by the École Polytechnique Fédérale de Lausanne (EPFL) and the World Bank Group (WBG), the dialogue also looked at social media's potential for the development agenda, and the challenges of assessing the credibility of gathered information and results.

A Digital Standardisation Tour 29 March 2021

The roundtable discussion, organised by the GIP as part of the series '12 Tours to Navigate Digital Geneva', showcased the work of the main Geneva-based organisations active in developing and setting digital standards, including the International Telecommunication Union (ITU), the International Standardisation Union (ISO), and the International Electrotechnical Commission (IEC). Although headquartered in Geneva, their standardisation processes take place at the national and international levels and through complex interaction among different stakeholders. The discussion touched upon the transparency and inclusivity of standardisation processes, and their consensus-based approach. The exchange also highlighted the need to assist the non-technical community, including diplomats, in following and understanding standardisation discussions.

On our radar: Global digital policy events in April

Let's look ahead at the global digital policy calendar. Here's what will take place in the next month worldwide. For more details and event updates, check our events page regularly.

April

5–7 APRIL, Cybertech Global 2021 (Dubai, UAE)

The 8th edition of Cybertech Global 2021 will discuss AI, advanced IoT, big data, the cloud, and blockchain, and will focus on a wide range of sectors, including finance and insurance, the health industry, and smart mobility. The highlight is an exhibitor's pavilion, and a chance for startups to showcase their new technology.

7–9 APRIL, Russian IGF (Moscow, Russia) (online)

Organised by the Coordination Center for TLD .RU/.РФ with the support of the Ministry of Communications and Mass Media, the Russian IGF will look at new technologies such as AI and their related ethical issues, data sovereignty, digital platforms and international cooperation, and cybersecurity myths and facts. The event will be held in a hybrid form, with speakers convening in Moscow and participants tuning in online.

22 APRIL, Girls in ICT 10th Anniversary (online)

The International Girls in ICT Day campaign is celebrating its 10th anniversary this year. To mark this date, the ITU has invited all stakeholders to organise activities on and around 22 April. There are currently 17 events organised in 10 countries, and stakeholders can still submit their own events to be added to ITU's calendar.

26 APRIL, World Intellectual Property Day 2021 (Geneva, Switzerland)

The theme of this year's World IP Day is 'IP & SMEs: Taking your ideas to market'. The World Intellectual Property Organization (WIPO), which is spearheading the campaign, invited stakeholders to organise their own events to 'help bring alive IP for SMEs'. Stakeholders are also invited to submit their events to the WIPO's calendar.

May

About this issue

Issue 58 of the *Digital Watch* newsletter, published on 7 April 2021 by the Geneva Internet Platform and DiploFoundation | Contributors: Katarina Anđjelković, Stephanie Borg Psaila (editor), Andrijana Gavrilović, Tereza Horejsova, Marco Lotti, Virginia (Ginger) Paque, Nataša Perućica, and Sorina Teleanu | Design: Aleksandar Nedeljkov, Viktor Mijatović, and Mina Mudrić, Diplo's CreativeLab. Get in touch: digitalwatch@diplomacy.edu

On the cover

Fit for travel. Credit: Vladimir Veljasević

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