GENEVA INTERNET PLATFORM
digwatch

NEWSLETTER

Issue 68, **April 2022**

In times of war

What's allowed, and what isn't?
A special report on Ukraine war

Pages 2–5

MARKETS

Parliament and the EU Council have reached a political agreement on the Digital Markets Act, which we unpack.

Pages 6–7

BAROMETER

Ukraine conflict aside, there were quite a few updates on the security, infrastructure, legal, and content policy fronts.

Pages 8–9

GENEVA

Human rights and e-commerce were quite high on Geneva's agenda in March. We summarise the main events.

Pages 10–11

UPCOMING

The calendar of global policy events for April is quite busy. Here are the upcoming discussions on our radar.

Page 12

To block or not to block?

As the war wages on in the streets of Ukraine, disinformation continues to spread online, with harmful consequences.

One of the main issues is how the war is being described. Russia is portraying it as a special military operation. Ukraine and most countries vigorously disagree and accuse Russia of downplaying its seriousness or denying it outright. What the West describes as the Bucha massacre is touted as fake Ukrainian propaganda by Russia.

Some countries have taken stiff action to curb the spread of disinformation. The EU, UK, and Canada banned Russian state media RT and Sputnik from broadcasting within their territories (Russian state-owned news agency TASS was not part of the ban). Russia took aim at RAI, CNN, CBS, Bloomberg, Euronews, and Google News, and others.

One country – Switzerland – took a different approach. 'Although these channels are tools of targeted propaganda and disinformation by the Russian Federation,' the Federal Council explained, 'countering untrue and harmful statements with facts is more effective than banning them.'

Switzerland's decision echoes what the European Federation of Journalists, the largest organisation of journalists in Europe, said in reaction to the EU's ban. 'The total closure of a media outlet does not seem to me to be the best way to combat disinformation or propaganda,' the EFJ's chief, Ricardo Gutiérrez, said. 'It is always better to counteract the disinformation of propagandist or allegedly propagandist media by exposing their factual errors or bad journalism'.

There are several issues here. First, neither of these approaches is achieving what it was hoping for. A government-led ban on media sources helps curb the spread of propaganda but places questionable limitations on media independence and the right to free expression (even though this is not absolute). The lack of clampdowns on known sources of state propaganda leaves the door wide open for disinformation to spread.

Second, beyond what European (or other) citizens should be protected from, a more important question is what other sources of information Russian citizens have access to.

As Jamie Wiseman of the International Press Institute's advocacy office, commented, Russia has starved its citizens of foreign media at a crucial time. Although disinformation should be counteracted by fact-checking, Russian citizens simply don't have the tools to do so since the media blackout started. British Prime Minister Boris Johnson's impassioned plea to Russian citizens, in their own language, will probably never reach the majority of Russian citizens.

Third, attributing Russia's media censorship to a reaction to the EU's and others' ban (from among other state-owned media) is questionable. While there was a good degree of angry reaction from Russia, it decided to block or throttle social media (and threatened to extend this to independent media), long before other countries imposed their bans on Russian state media.

The UN Human Rights Council made headway last week when the draft resolution on countering disinformation was adopted (without a vote) at the end of its 49th session, on 1 April, with very few countries disassociating themselves from the text (Russia was suspended from the human rights body a few days later).

If anything, there's now widespread recognition that, citing China, disinformation is 'a common enemy of the international community'. Ongoing disinformation campaigns will not suddenly disappear, but there's now a growing understanding among countries of what's allowed and what shouldn't be, even in times of war.

Russia vs Meta

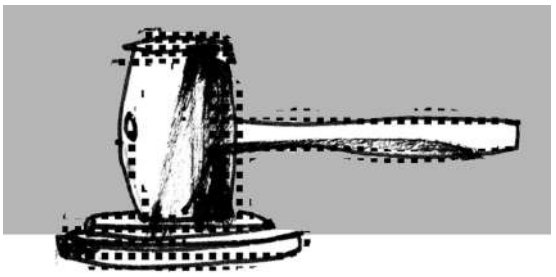
Hate speech – or what is often referred to in legal texts as incitement to violence – is an animal of a different colour. While disinformation is largely harmful, many shades of hate speech are (usually) considered illegal.

So when Meta asked its content moderators to temporarily allow Facebook and Instagram users in the region to call for violence against Russian soldiers on 11 March, Russia's reaction to ban Facebook and Instagram was to be expected. Even though a few days later Meta clarified that it would prohibit calls for the death of a head of state (but still allow calls for violence), Russia's ban was confirmed by a Russian court.

'We are issuing a spirit-of-the-policy allowance to allow T1 violent speech that would otherwise be removed under the Hate Speech policy,' Meta informed its content moderators in an email that was leaked to the press. This instruction refers to speech 'when: (a) targeting Russian soldiers, EXCEPT prisoners of war, or (b) targeting Russians where it's clear that the context is the Russian invasion of Ukraine (e.g., content mentions the invasion, self-defence, etc.)'.

The text in Meta's email looks like a page from a country's civil or criminal code. Yet, Meta is not part of the legislative branch of any country nor is its policy a part of the law of any land. It begs the question: Should we start looking at social media forums as public spaces, requiring normative rules enforceable by public authorities? Or should they continue to be managed and policed by members of the private sector, as the creators of these spaces? Or should there be a different formula that places these spaces somewhere in between? Obviously, governments, and the industry are at odds.

Decisions taken over content affect a wide range of people. In this case, posts against Russian soldiers from Armenia, Azerbaijan,



Estonia, Georgia, Hungary, Latvia, Lithuania, Poland, Romania, Russia, Slovakia, and Ukraines will be allowed, affecting both the authors and those against whom the hate speech is directed.

There's also an issue of transparency. The decisions of Meta's content managers are based on two things: the company's community standards (the policy), and the company's guidelines on how to interpret the standards. The former is public information; Meta's website includes a changelog to show the changes from one iteration of the standards to the next. The latter, the company guidelines, are not public, but in this case, had to be leaked to the press for us (and the Russian government) to learn about them.

The laws of the land are public, the world over. The way the law is developed is also a public matter, preserved through parliamentary records. The same goes for case law (with some exceptions).

If companies want to continue (or regain governments' trust to continue) to self-manage these spaces, they need to do more to appease concerns. Although some might say it could encourage abusers, making the guidelines publicly available on a website will not, by itself, fuel people to post violent messages.

On its own, transparency won't be enough to solve the issues plaguing content policy. Still, at least until governments and companies get there, users can have clear signposts along the way.

AI and facial recognition during wartime

When the news broke out that Ukraine was using Clearview AI facial recognition technology (FRT) to identify dead Russian soldiers, the press sounded an alarm. 'Critics say the use of facial recognition in war zones is a disaster in the making,' Forbes' associate editor Thomas Brewster wrote.

The number of times Clearview AI has been sued in courts around the world and slapped with hefty fines for privacy breaches is enough to make people uneasy, especially when it's used during a war.

To be clear, the only known use of FRT by Ukraine's government has been for non-warfare purposes. In an interview, the country's Deputy Prime Minister Mykhailo Federov explained that Ukraine has been using Clearview AI to find the social media accounts of deceased Russian soldiers to notify their families to collect the body.

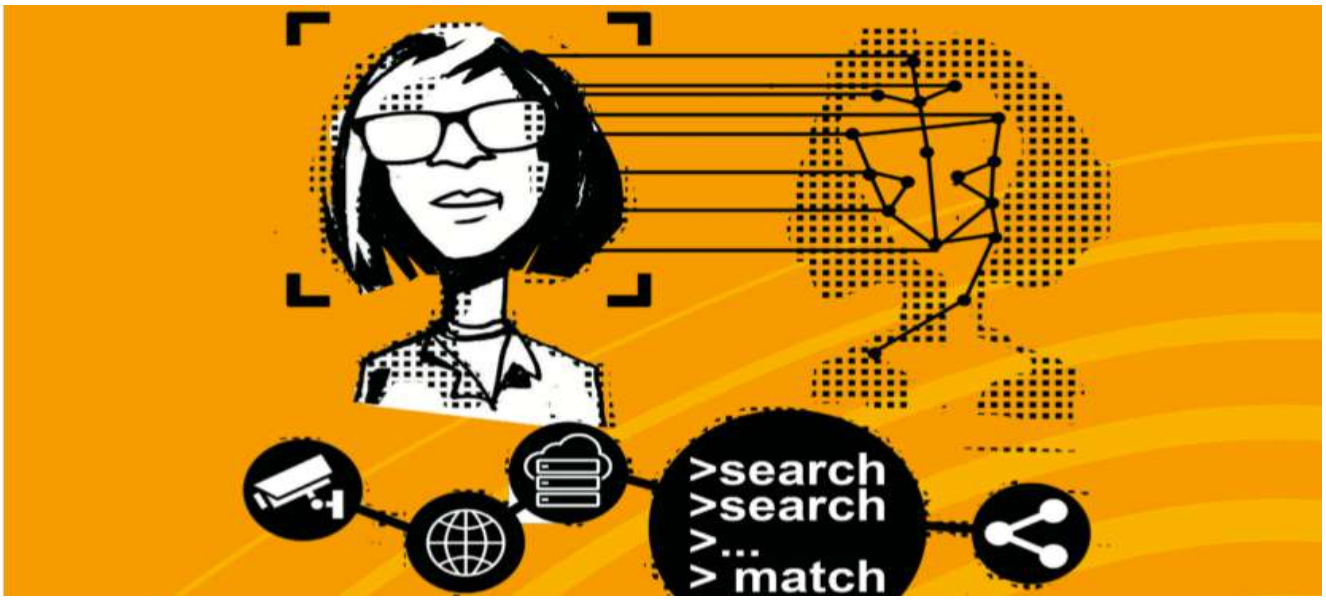
In a tweet, Federov added that the facial recognition software 'autodial(s) RU subscribers to tell the truth about the war'. His tweet referred to 'Face ID', presumably Apple's FRT software, used alongside Clearview AI.

FRT is a bit like fire. It has undeniable useful applications. But add FRT's proclivity for

misidentification, no matter how slight, and it immediately becomes dangerous. As Albert Fox Cahn, founder of the Surveillance Technology Oversight Project told Forbes, 'when facial recognition makes mistakes in peacetime, people are wrongly arrested. When facial recognition makes mistakes in a war zone, innocent people get shot.'

The problem, therefore, is what comes next. If any side on the frontlines, no matter whom, starts using FRT for purposes well beyond informing Russian families about their loved ones' deaths, concerns increase exponentially.

The identification accuracy rate of 99.85% described by ClearView AI's CEO, Hoan Ton-That, doesn't do much to assuage fears about the other 0.15%. Anything short of 100% can be disastrous for anyone in FRT's line of sight.



The cost of cyberwar for other countries

Although Ukraine is the epicentre of the ongoing war, other countries are often collateral damage from cyberattacks on their critical infrastructures and businesses.

For instance, European government officials helping Ukrainian refugees were targeted with phishing emails orchestrated to originate from the email address of a compromised Ukrainian armed service member. Cybersecurity company Proofpoint explained that the characteristics of this attack are very similar to tactics employed by Ghostwriter (or UNC1151), a hacking group operating from Belarus.

Beyond the obvious harm from the malware contained in the phishing emails, Proofpoint thinks that the aim is to spread an anti-refugee sentiment among European countries and ultimately decrease Western support for Ukraine. 'This approach is a known factor within the hybrid warfare model employed by the Russian military and by extension that of Belarus.'

In the USA, the FBI detected network scanning activity coming from different Russia-based IP addresses, targeting the US energy sector, according to an FBI advisory obtained by the press. Companies from other sectors, including the defence and financial services industries, were also scanned. Scanning activity is common, but that scanning has intensified since the start of the conflict in Ukraine supports the hunch that the Russian state might be responsible. US President Joe Biden also told business leaders to beef up their security. Addressing a quarterly business meeting, Biden warned that 'based on evolving intelligence, Russia may be planning a cyberattack against us… The magnitude of Russia's cyber capacity is fairly consequential, and it's coming.'

The Kremlin has dismissed these warnings. 'Unlike many Western countries, including the United States, Russia is not engaged in state banditry,' the Kremlin spokesman told reporters.

So what's fair to expect? Recent history speaks for itself. Last year (before the war started), in just a few weeks, a spate of malware attacks crippled the operations of US oil and gas supplier Colonial Pipeline, meat-producing company JBS, and Ireland's health network. Together with the SolarWinds hack, which the USA attributed to Russia, the cyberattacks were a precursor to US-Russia cybersecurity talks launched in Geneva in June 2021 (now on hold, possibly indefinitely). If all of this happened in a time of peace, CISA's advice to shield up is to be heeded.

Gatekeepers, beware:
The EU's Digital Markets Act is around the corner

At the beginning of this year, we wrote a side-by-side recap of two pieces of draft legislation – the Digital Services Act (DSA), and the Digital Markets Act (DMA) – that will impact consumers, businesses, and Big Tech in important ways.

When we wrote our article in January, the European Parliament had just approved the texts that would serve as parliament's mandate to negotiate with EU governments. Fast forward three months, and after an intensive trilogue (three-way talks as part of the ordinary legislative process), on 24 March, the parliament and the Council of the EU reached a political agreement on the first of the texts, the DMA.

The two main issues

Since the beginning of the DMA's legislative journey, which started in December 2020, the two biggest questions have been:

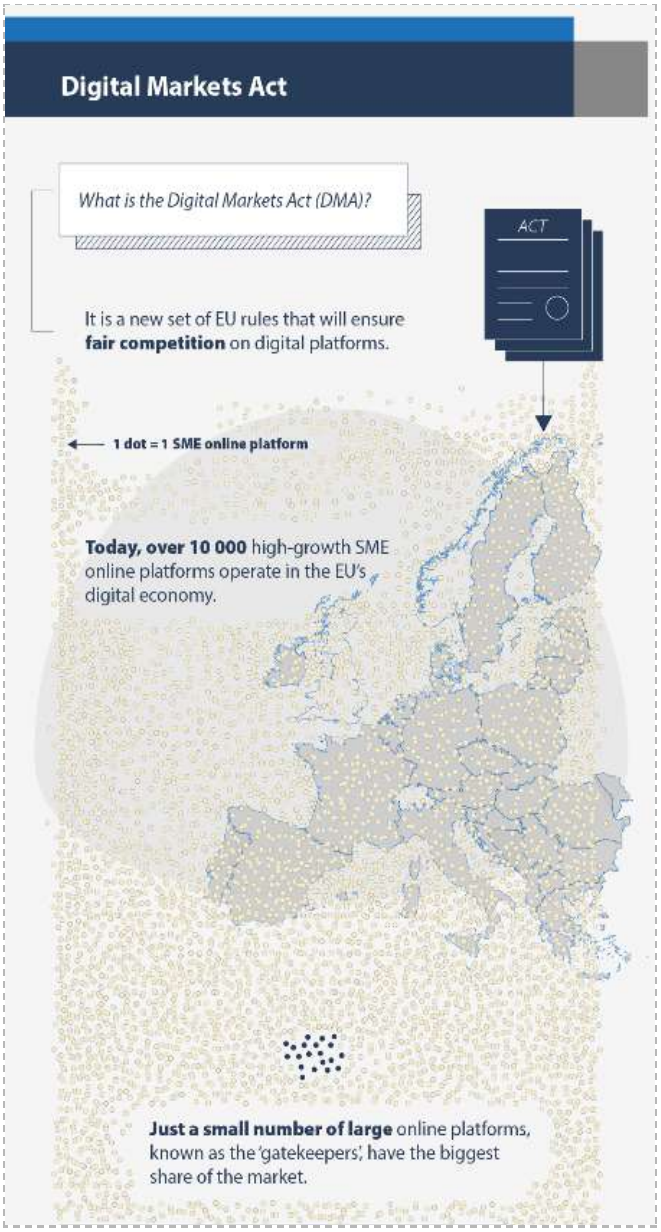
(a) Which companies will fall under the DMA?
(b) What obligations will it impose on them?

The reason these two are connected is that the law will be telling companies: If you've been successful enough to find yourself offering a core service to EU users, you might be designated a gatekeeper. That title comes with a set of obligations that must be followed.

Who are the potential gatekeepers?

The definition of gatekeeper (in Chapter II of the draft law) relies on a mix of qualities and numbers, which the European Commission will use to decide whether to confer gatekeeper status on a company.

First, the company will need to have significant market power. Throughout the negotiations, the needle had been oscillating between companies earning at least €6.5 billion in turnover in the EU (or a market value of €65 billion), and those earning at least €8 billion in turnover (or valued at €80 billion). In the end, based on what the EU Council and the parliament announced (no updated text was published), the agreed thresholds are at least €7.5 billion in turnover (or a market value of at least €75 billion).



A section of the updated official Digital Markets Act infographic, which includes a visual representation of gatekeepers in the context of the EU's digital economy. Another section from the infographic is on the next page. Source: Council of the EU

Second, the company also must be in control of one or more core services, such as social networks (think of Meta), search engines (think of Google), marketplaces (think of Amazon), and app stores (think of Apple).

You'd be forgiven to think that the legislators had a preconceived list of companies they wanted to target.

In fact, experts say that they most likely used the so-called backward induction process: 'The Commission had a rough idea of the companies that the DMA should capture, it then crafted the thresholds accordingly, to be sure the bigger players would be included.'

Negotiators would have had a similar list, including US government officials who had circulated an eight-point policy document among key EU legislators to avoid raising the thresholds, lest the DMA might target exclusively large US tech firms.

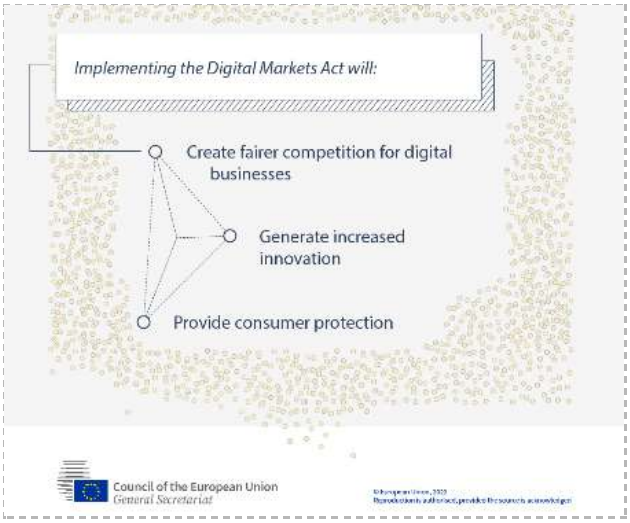
So what if a company wants to turn down the Commission's title of gatekeeper? There seems to be no change from the original version (see Article 4.1): A company can challenge the designation by asking the Commission to revisit its decision.

What are the obligations imposed by the DMA?

In the absence of an updated legal text, we'll rely on the EU Council's summary:

Gatekeepers will have to:

- ensure that users have the right to unsubscribe from core platform services under similar conditions to subscribing
- for the the most important software (e.g. web browsers), not require any specific software by default upon installation of the operating system
- ensure the interoperability of their instant messaging services' basic functionalities with similar services
- allow app developers fair access to the supplementary functionalities of smartphones (e.g. NFC chip)



- give sellers access to their marketing or advertising performance data on their platform
- inform the European Commission of their acquisitions and mergers

But they can no longer:

- rank their own products or services higher than those of others (self-preferencing)
- reuse private data collected during a service for the purposes of another service
- establish unfair conditions for business users
- pre-install certain software applications
- require app developers to use certain services (e.g. payment systems or identity providers) in order to be listed in app stores

Non-compliance will attract hefty fines. Companies can be fined up to 10% of their total worldwide turnover (as per the original draft, Article 26), going up to 20% in case of a repeated offence (as suggested by Parliament).

What happens next?

It won't be long now before the DMA becomes law. What's left is the technical refinement, and a final nod by parliament and the EU Council. But that's not the end for companies. The DSA, which will also impact consumers, businesses, and Big Tech in important ways, is also on its way. We'll unpack that when the time comes.

Digital policy developments that made headlines

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

Increasing relevance

Global architecture

The UN Ad Hoc Committee on Cybercrime adopted a roadmap outlining the next steps in the negotiations on a new treaty. The UN Open-Ended Working Group (OEWG) Developments in the Field of Information and Telecommunications in the Context of International Security held its second substantive session. *Visit the UN OEWG 2021-2025 page for more details.*

A group of internet experts proposed a set of principles for internet infrastructure governance sanctions.

The UN Secretariat convened an Expert Group Meeting to consider how the Internet Governance Forum can contribute to advancing digital cooperation.

Same relevance

Sustainable development

The International Telecommunication Union (ITU) launched a Partner2Connect online pledging platform and an action framework to advance universal connectivity and digital transformation.

Saudi Arabia and Egypt signed an agreement to cooperate on digital transformation.

Increasing relevance

Security

A distributed denial of service attack took down several government websites in Israel. Nvidia, Microsoft, Octa and Samsung were hacked by the Lapsus$ cybercrime group. Arrests connected to the cases were made in the UK.

The Online Safety Bill was introduced in the UK Parliament. In the USA, a bipartisan coalition of state attorneys general launched an investigation into TikTok's effect on children's well-being. A UK High Court greenlighted a class-action privacy lawsuit against TikTok over its handling of children's data.

Ukraine conflict: More cyberattacks and vulnerabilities exposed (see our 'Ukraine conflict: Digital and cyber aspects' page).'

Same relevance

Digital rights

The Irish data protection authority (DPA) fined Meta €17 million over GDPR breaches. Sri Lanka passed a new data protection law. Saudi Arabia postponed the enforcement of its new data protection law until 17 March 2023.

Infrastructure


Increased relevance

Intel announced major investments in the research, development, and manufacturing of semiconductors in the EU. The semiconductor industry also featured among President Biden's priorities in his State of the Union Address.

The World Telecommunication Standardization Assembly agreed on the mandates of the ITU Telecommunication Standardization Sector's study groups for the 2022–2024 study period and reviewed a series of resolutions and recommendations.

E-commerce and the internet economy


Same relevance

US President Joe Biden instructed national agencies to develop regulations on digital assets. UK's Financial Conduct Authority warned operators of cryptocurrency ATMs to shut them down.

Ukraine conflict: More sanctions affected e-commerce and trade (see our 'Ukraine conflict: Digital and cyber aspects' page).

Content policy


Increasing relevance

Ukraine conflict: Russia adopted a new disinformation law carrying penalties for spreading fake news related to its 'military operation' in Ukraine and banned Meta's social networks Facebook and Instagram over a change in policy that allows Ukrainians to call for violence against Russian soldiers. *More on pages 2–5.*

Ukraine conflict: The Security Service of Ukraine destroyed five bot farms, claiming the farms were carrying out information sabotage on Russia's behalf.

Jurisdiction and legal issues


Increasing relevance

EU institutions reached an agreement on the DMA. *More on pages 6–7.*

The EU and USA agreed 'in principle' on a transatlantic data privacy framework.

New technologies


Increased relevance

Civil society groups called on the EU to ban predictive AI in policing and criminal justice. The European Parliament's Special Committee on AI in the Digital Age concluded its work with a set of final recommendations. The US National Institute of Technology called for a socio-technical approach to mitigate bias in AI.

Germany allocated €76.3 million to the QSolid quantum computer project. The Weizmann Institute of Science announced the launch of Israel's first quantum computer.

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.

28 February – 1 April 2022 | 49th Session of the Human Rights Council

Addressing the council at the start of the session, UN Secretary-General Antoinio Guterres sounded a stark warning on how digital technology is being used to trample on human rights. 'Digital technology is the Wild West for human rights', Guterres warned, explaining how censorship has been normalised, and how AI enables algorithms to discriminate. His comments echo a similar warning he made earlier this year, but added in his HRC address that 'The internet must be treated as a global public good.' Guterres also made reference to his proposal for a Global Digital Compact, which he made in his 2021 report Our Common Agenda, and which will be tackled in the Summit of the Future in 2023. UN High Commissioner for Human Rights Michelle Bachelet also cautioned against disinformation which is corroding societies, and encouraged states to take strong action to ensure that digital technology advances rights everywhere, rather than undermining them.

When it comes to reports, the dialogue with Special Rapporteur on the Right to Privacy Ana Brian Nougrères, on 10 March, shed light on her report Privacy and Personal Data Protection in Ibero-America: A Step Towards Globalisation? Brian Nougrères explained how the cooperation mechanism between Ibero-America and the EU, which has been developing for two decades, can serve as a model for collaboration, and possibly a first step towards the global harmonisation of privacy and personal data protection rules. *Read our report from this event*.

As for resolutions adopted at the end of the 49th session, the resolution on countering disinformation (adopted without a vote) called on states to refrain from spreading or harbouring disinformation campaigns, and to ensure that any responses to tackling disinformation comply with international human rights law. A high-level panel discussion will take place at the Human Rights Council's next session in June–July (*more on page 3*). The resolution on the rights of the child (adopted without a vote) mandated the Office of the United Nations High Commissioner for Human Rights to organise its annual full-day meeting on the rights of the child in 2023 on the theme, 'Rights of the child and the digital environment'.

UN Secretary General Antonio Guterres addressing the 49th Session of the Human Rights Council. Source: video capture

17 March 2022 | Geneva presentation of the UNDP special report on human security

A new report by the UNDP, New Threats to Human Security in the Anthropocene: Demanding Greater Solidarity, shows that people's sense of safety and security is at a low in almost every country. (If you're wondering what 'anthropocene' means, it's a proposed concept to describe an epoch in which humans become central drivers of change to our planet, and radically alter the earth's biosphere through challenges and threats to human security).

Speaking at a discussion organised by the Geneva Centre for Security Policy (GCSP) and the UNDP Office in Geneva, to mark the report's launch in Geneva, GCSP Director Ambassador Thomas Greminger stressed that a comprehensive approach to security which integrating human security into the mainstream of security policy has never been more critical.

UNDP Human Development Report Office (HDRO) Director Pedro Conceição referred to some of the report's findings, which showed that more than six out of seven people already felt insecure during the pre-pandemic period. UNDP Geneva Director Agi Veres commended the report as a useful addition to the traditional global debate on security. Geneva Internet Platform Head and Diplo Director Jovan Kurbalija said that the digital infrastructure has become critical for today's society. After the stress test imposed by COVID-19, the internet is again on trial with the war in Ukraine *(more on pages 2–5)*.

Deputy Permanent Representative of Tanzania Hoyce Temu said that the report has emphasised the need to give women a stronger voice.

The war in Ukraine is a terrible blow to multilateralism, Permanent Representative of Switzerland to the UN Ambassador Jürg Lauber said, and the UNDP report is also an appeal to renewal of multilateralism and international cooperation. People, governments, and civil society can mobilise resources very quickly. Mr Lauber stressed that: 'We need to collectively adopt a similar sense of urgency and use the strategy of solidarity to respond to interconnected threats faced by people and the planet at the global scale.'

21 March 2022 | High-level seminar: Making electronic commerce work for development by connecting the dots

The COVID-19 pandemic has increased the uptake of e-commerce all over the world. However, developing countries face many impediments that prevent businesses from taking advantage of the digital transformation.

This event, organised by UNCTAD, discussed UNCTAD's eTrade Readiness Assessments and how developing countries can make use of the assessments to enhance the implementation of concrete policy recommendations.

According to Didier Chambovey, ambassador and permanent representative of Switzerland to the WTO, the accelerated shift to digital activity has triggered a transformational impact on production, consumption, and trade patterns. Chambovey highlighted that 'While digital connectivity is a key tool to promote sustainable and inclusive growth, it has led to asymmetrical development throughout the world.'

Rebeca Grynspan, secretary-general of UNCTAD, honoured the role of Switzerland as a core partner in e-commerce and the digital economy. Switzerland supports UNCTAD's assistance to member states seeking to build their digital economies; it is very beneficial that these countries can benefit from Switzerland and Geneva, centres of excellence in digital development.

What to watch for: Global digital policy events in April

Let's look ahead at the global digital policy calendar. Here's what will take place around the globe. For more events, visit the Events section on the Digital Watch Observatory.[link]

11–12 April **SEE 10: RIPE NCC Regional Meeting**	RIPE NCC's regional meeting for South East Europe (SEE) 10 will be hosted by the Academic and Research Network of Slovenia (ARNES) and the Slovenian Network Operators Group (SiNOG) on 11–12 April in Ljubljana, Slovenia. The regional forum is an opportunity for network engineers and other technical staff to share knowledge and experiences, as well as to identify areas for regional cooperation.
12–13 April **IAPP Global Privacy Summit 2022**	Every year, the International Association of Privacy Professionals (IAPP) gathers the privacy professionals community to network, provide education opportunities, discuss critical updates from the who's-who of the field, and discover new solutions and best practices. This year's summit will be an in-person event in Washington, DC on 12 and 13 April. Topics include international data transfers, privacy operations management, online advertising, data breach/loss, and privacy metrics.
12–14 April **#DRIF22 - Digital Rights and Inclusion Forum**	DRIF22 is a platform for African communities of practice around privacy, affordable Internet, gender and ICTs, disability rights and ICTs, health surveillance during COVID-19 times, internet shutdowns, and similar themes. This years' edition will be held online 12–14 April, after which a series of in-person consultations will take place across 17 African countries.
21 April **POLITICO's AI and Tech Summit**	The 5th edition of POLITICO's AI and Tech Summit will showcase special discussions on issues regarding key legislative files such as the Data Act and the Digital Services Act (DSA), data protection, and how to best harness the potential of AI in areas such as cybersecurity, healthcare, and gaming. The Summit will take place in Brussels on 21 April.
25–29 April **UNCTAD e-commerce week**	The United Nations Conference on Trade and Development (UNCTAD), in collaboration with eTrade for all and other partners, will host its annual eCommerce Week. This event will take place in Geneva and online 25–29 April 2022, under the theme 'Data and Digitalization for Development.' The focus will be on data, cross-border data flows, and the crucial role they play in economic and social development. We'll be reporting from this event, so stay tuned.

About this issue: Issue 68 of the Digital Watch newsletter, published on 10 April 2022 by the Geneva Internet Platform and DiploFoundation, under a CC BY-NC-ND 4.0 licence | Contributors: Stephanie Borg Psaila (lead author), Andrijana Gavrilovic, Kristina Hojstricova, Jana Misic, Virginia (Ginger) Paque, Sorina Teleanu | Design: Viktor Mijatović | On the cover: In times of war. Credit: Vladimir Veljašević | Feedback? Drop us a line.

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