



Ad Hoc Committee on Cybercrime



Agreement on UN cybercrime convention elusive

Pages 4-5

DIGITAL POLICY SNAPSHOT

AI governance and cybersecurity dominated news coverage in February.

Pages 2-3

IN FOCUS

Is Neuralink's first human brain chip implant a scientific breakthrough? Or is it just sensationalism?

Page 6

IN FOCUS

In the backdrop of the 2024 elections, February saw a notable increase in efforts to mitigate misinformation's impact on the electoral process.

Page 7

IN FOCUS

Germany published its first Strategy for International Digital Foreign Policy, putting digital as a strategic priority.

Page 8

Snapshot: The developments that made waves

Global governance

Co-facilitators have [delineated the possible elements](#) of the Global Digital Compact (GDC).

AI governance

China and Russia have decided to [work together on the military implementation of AI](#). The US Department of Justice [appointed its first Chief AI Officer](#), while Japan initiated a [comprehensive legislative push for AI](#) in 2024. The EU Commission has [established a working group](#) comprising officials from member states to tackle inquiries about the AI Act. The UK's AI minister has offered to [work with the EU on AI policy and copyright issues](#).

OpenAI's CEO has advocated for the [UAE policy environment as a potential global AI regulatory sandbox](#). Meanwhile, Nvidia's CEO emphasised the imperative for [countries to establish their independent AI infrastructure](#).

French MPs expressed [concerns over the Mistral AI and Microsoft partnership](#), citing worries about competition and data sovereignty in the cloud sector.

OpenAI [introduced Sora](#), an AI tool capable of generating videos from text commands. The company also introduced a new [personal memory feature for ChatGPT](#), which aims to improve the chatbot's ability to remember user preferences, conversations, and other relevant information. Microsoft has announced [principles to foster innovation and competition within the field of AI](#). Google plans to [relaunch the Gemini AI image generation tool](#) after a temporary pause to fix inaccuracies in historical depictions generated by the app.

Technologies

As part of its New Growth 4.0 strategy, the South Korean government plans to [introduce cloud services powered by quantum computing](#). The World Semiconductor Council (WSC) has urged India to [reconsider its proposed tariffs on digital e-commerce and data transfers](#), cautioning that such measures may impede the growth of India's chip design sector.

Infrastructure

China has [launched a satellite](#) for testing 6G technology. The USA and its allies have endorsed shared [principles for developing 6G technology](#). The [EU Gigabit Infrastructure Act](#) will end intra-EU call charges by 2029, upholding the voluntary tacit approval principle. The [Houthi threat to critical submarine cables](#) in the Red Sea raised concerns. The European Commission has unveiled a [package to boost the innovation, security, and resilience of digital infrastructures](#) in Europe.

Cybersecurity

The Netherlands revealed a covert [Chinese cyberespionage campaign within its military network](#). An intelligence advisory highlighted the [infiltration of US critical infrastructure by China-linked Volt Typhoon hackers](#). Simultaneously, [leaked documents revealing China's alleged offensive cyber tactics](#) surfaced.

An analysis by Microsoft and OpenAI [highlighted how threat actors are currently using large language models \(LLMs\)](#). The National Institute of Standards and Technology (NIST) [released the Cybersecurity Framework 2.0](#), which aims to help all organisations manage and reduce risks.

International law enforcement agencies achieved notable success by [disrupting the operations of the LockBit ransomware gang](#). However, this brief respite was overshadowed by the [gang's comeback](#), shortly after. A collective warning issued by the FBI, CISA, and HHS, cautioned against the [ALPHV/BlackCat ransomware specifically targeting the US healthcare sector](#). The advisory comes after a [BlackCat cyberattack on UnitedHealth Group](#), leading to an outage affecting Change Healthcare, a pivotal payment exchange platform in the US healthcare system.

The [concluding session of the Ad Hoc Committee on Cybercrime ended](#) with no consensus. *Read more on [pages 4 and 5](#).*

The Pall Mall Process, a [multistakeholder initiative to tackle spyware](#), was launched at a

conference convened by the UK and France with representatives from 35 nations, alongside major tech companies like Google, Microsoft, and Meta.

Human rights

President Biden issued an executive order authorising the attorney general to [prevent the large-scale transfer of US citizens' personal data](#) to 'countries of concern' such as China, Russia, North Korea, Iran, Cuba, and Venezuela. Portugal mandated telecom companies to [ensure equal access for individuals with disabilities](#), requiring tailored equipment, software, and tariffs effective from 28 June 2025.

Legal

Elon Musk is suing OpenAI, claiming a [departure from the organisation's founding principles](#) of prioritising technology for humanity over profits, which OpenAI leadership [refuted](#). OpenAI has requested a federal judge to [dismiss parts of the New York Times' copyright lawsuit](#) against it, claiming that the newspaper used misleading prompts, causing ChatGPT to generate misleading evidence. The US Patent and Trademark Office (USPTO) issued [guidance for inventions assisted by AI](#), emphasising human contributions for patent eligibility

Internet economy

A [draft of the digital trade protocol to the African Continental Free Trade Area \(AfCFTA\)](#) has been circulated. Countries agreed to [extend a moratorium on placing tariffs on digital goods](#) at the WTO 13th Ministerial Conference (MC13). The European Commission imposed a EUR [1.8 billion fine on Apple](#) for restricting music streaming services from offering alternative payment options outside its App Store. Bitcoin [experienced a rally in price](#) due to the approval of exchange traded funds (ETF) in the USA and a planned reduction of miner rewards.

Development

The EU [adopted a new 'right to repair' law](#), while China pledged to [recycle half of its e-waste by 2025](#). China also [launched a program to boost national digital literacy](#).

Nigeria initiated a [nationwide effort to expand internet access](#). Sudan has experienced a [widespread internet shutdown](#) affecting over 14 million people, while Pakistan's [election day mobile service suspension](#) raises digital rights concerns.

The UAE unveiled a USD [200 million technology fund](#) for developing nations. A USD [9 billion commitment to ITU's universal connectivity drive](#) is set to benefit millions.

Sociocultural

The EU has enacted the [Digital Services Act \(DSA\)](#), fortifying online safety and governance. An [investigation into TikTok](#) has been launched under the DSA. The EU Parliament has adopted [rules to enhance trust and transparency](#) in election campaigns. Canada's [Online Harms Act](#) has set its sights on harmful content and internet giants.

THE TALK OF THE TOWN – GENEVA

On 20 February, the World Health Organization (WHO) [launched the Global Initiative on Digital Health \(GIDH\)](#), a WHO-managed network that augments resources in country-led digital health transformation by fostering knowledge sharing and collaborations. The initiative aims to assess and prioritise country needs, build capacity to encourage local developments and accelerate the achievement of strategic goals listed in WHO's [Global Strategy on Digital Health 2020-2025](#).

The International Labour Organization (ILO) hosted the research seminar [Behind the AI Curtain: The Invisible Workers Powering AI Development](#). The seminar shed light on the significant amount of human labour, often from developing countries, behind the advancement of AI technologies and the precarious working conditions such labourers face. The seminar presented research insights on the much-needed ethical considerations for hidden human labour and called on policymakers and labour advocates to protect the rights of these invisible AI workers.

Agreement on UN cybercrime convention elusive

The UN's [Ad Hoc Committee on Cybercrime](#) (AHC) met in New York from 29 January to 9 February 2024 for its concluding session after 2 years of negotiations. However, significant progress was lacking, particularly regarding the convention's scope. Additional meetings were deemed necessary, though some states expressed concerns about resource strain.

Negotiations were split between formal sessions and closed-door informal meetings that focused on sensitive issues but reduced transparency and excluded input from the multistakeholder community.

In the last days of the concluding sessions, there was increased pressure from [civil society and industry](#), as well as [cybersecurity researchers](#).

Issues with the draft convention that still require resolution include:

Scope of the convention and criminalisation

One main unresolved issue is whether the cybercrime convention should cover all crimes committed via ICT or not. Canada [made a proposal](#), supported by 66 states, to insert a broad wording of the actions that may fall within the scope of the convention.

At the same time, Russia [insisted](#) on more extensive measures against terrorism and criticised the draft, highlighting that 'many articles are simply copied from treaties that are 20 years old.' In the same vein, Iran, Egypt, and Kuwait see the primary mandate of the AHC to elaborate a comprehensive international convention on the use of ICT for criminal purposes and see the inclusion of human rights regulations and detailed international collaboration as duplication of already existing international treaties.

Civil society, private entities, and academia stressed limiting the convention's scope to protect rights and cybersecurity.

Human rights and safeguards

Delegations also struggled with human rights and safeguards provisions. Iran proposed a model similar to the UN Convention against

Corruption, omitting explicit human rights references, but didn't receive support from many other delegations. Egypt and others criticised repetitive human rights provisions in the text and questioned the singling out of the principle of proportionality in Article 24.

There were debates over including 'legality' alongside proportionality, with Brazil's proposal finding support from Ecuador.

As a result, both articles remain without text in the [further revised draft text of the convention](#).

Transfer of technology and technical assistance

The topic of technology transfer arose in Articles 1 and 54 of the convention. While African countries pushed for its inclusion in both, the USA advocated for it to be solely in Article 54.

Disagreements persisted over the language in Article 54(1), with the USA and several other delegations proposing additional terms opposed by several African countries and others. In particular, African countries and others opposed inserting 'voluntary' before 'where possible' and 'on mutually agreed terms' in the context of how capacity building shall be provided between states. They argued that it would undermine the purpose of the provision in ensuring effective assistance to developing countries. Eventually, the USA withdrew its suggestion, leaving room for further negotiation on the draft text of the convention.

Scope of international cooperation

Delegations held differing views on cooperation regarding electronic evidence, particularly in Articles 35(1)(c), 35(3), and 35(4). The draft convention allowed countries to collect data across borders without prior legal authorisation. However, several countries, including New Zealand, Canada, and the EU, raised concerns about the broad application of Article 35, fearing it might lead to the pursuit of non-criminal activities. On the other hand, states like Egypt, Saudi Arabia, and Iran called for the removal of Article 35(3) altogether.

In focus

New Zealand also proposed a non-discrimination clause in Article 37(15) on extradition to prevent unfair grounds for refusing cooperation. However, member states couldn't agree on the language and left this open.

Delegations held debates about Articles 45 and 46 around changing 'shall' to 'may', potentially providing states with the option rather than the obligation to cooperate. While some supported this change, others, including Egypt and Russia, preferred to retain 'shall' for robust cooperation.

The [revised draft text of the convention](#) includes both options in brackets, reflecting the ongoing discussions.

Preventive measures

Several delegations were confused about the term 'stakeholders' in Article 53 regarding preventive measures. Egypt proposed its removal unless clearly defined, but the USA disagreed. The revised draft replaced 'stakeholders' with 'relevant individuals and entities', but consensus on the paragraph is pending.

Additionally, disagreement persisted in Article 53(3)(h) on mentioning 'gender-based violence', with some advocating for its deletion.

Ultimately, the term remained. In Article 41, concerning the 24/7 network, India proposed incorporating requirements for prevention by law enforcement entities, supported by Russia, Kazakhstan, and Belarus, but opposed by the USA, UK, and others.

What's next?

Delegations agreed to postpone the final decision, with the chair's [further revised draft text of the convention](#) available on the AHC's website. Future meeting dates will be announced soon.

Despite progress on several issues behind closed doors, reaching a consensus on the cybercrime convention before the UN General Assembly remains uncertain. Ongoing non-public negotiations between delegations could potentially expedite the process. We will continue to monitor the negotiations and, in the meantime, you can discover more through our [detailed reports from each session generated by DiploAI](#).

*A longer version of this blog is [available](#) on the *Digital Watch Observatory*.*



Image credit: UN Web TV

Musk's brain chip: scientific breakthrough or sensationalism?

Elon Musk's brain-chip startup, Neuralink, has allegedly [successfully](#) implanted a brain chip in a human patient who has since fully recovered. Musk disclosed that the patient can now control a computer mouse using their thoughts alone.

Understanding Neuralink's technology

The technology [behind](#) Neuralink, known as 'the Link', involves a coin-sized brain chip surgically placed under the human skull. This implant, connected to neural threads distributed throughout various areas of the brain controlling motor skills, receives and decodes neural signals. In simple terms, it measures brain activity and interprets it as actions.

Neuralink envisions a future where individuals can manipulate keyboards and mice using only their thoughts. The technology's ability to decode brain activity as actions holds promising potential for individuals with limited mobility or speech impairments.

Neuralink in perspective: a look at BCIs

Neuralink's chip is [not the first device implanted in a human brain](#). Currently, more than 40 brain-computer interface (BCI) [trials are underway](#) in the USA alone. More than [200,000 people worldwide](#) already use a BCI, primarily for medical reasons. The most well-known common devices of this type are hearing aids that help people with hearing impairments to hear better.

Still, Elon Musk's announcement made quite a stir among the scientific community and the public. Musk has a history of making bold promises, but his track record in fulfilling them is inconsistent.

Despite Musk's assurance of a complete patient recovery without any side effects, the medical community remains cautious due to the lack of substantial evidence supporting his claims.

Human trials and safety concerns

Though [approved](#) by the US Food and Drug Administration (FDA), the beginning of human trials has [triggered concerns](#) about volunteer safety due to the scarcity of details about the trial, transparency, and information sharing.

From a legal standpoint, Neuralink is in the [clear](#), as the FDA does not require reporting of early feasibility studies. However, some medical experts [caution](#) that the complexity of the surgery involved in opening up the brain raises ethical considerations. Inserting a device into a living human being, especially someone with medical problems, [demands more comprehensive](#) reporting and transparency. Current (human) research subjects, all potential future research subjects, the medical community, and the public at large deserve to know more.

Neuralink's journey into BCIs has not been without controversy. Initial experiments involved subjects such as monkeys and pigs, with a 2021 [viral video](#) showcasing a chimpanzee playing the classic video game Pong using mind control.

However, behind the scenes, the company has come under fire [for a significant number](#) of euthanisations of primates that underwent medical trials. Veterinary records of these animals demonstrated complications arising from surgically implanted electrodes, raising concerns about the well-being of the subjects involved.

Brain chips also raise controversies regarding privacy and surveillance. The primary challenge is ensuring that companies developing this technology do not have access to our thoughts.

While Neuralink's developments hold promise for potential human applications, the lingering question remains: What are the consequences for people? The technology's long-term impact on human subjects remains uncertain. Neuralink's so-called breakthrough must be approached with caution, and we should await tangible results that demonstrate that it's not just another marketing trick.

2024 Elections: The misinformation battle and the role of social media platforms

All eyes on AI during the 2024 elections

In 2024, the global stage is set for a plethora of elections, [with at least 83 slated worldwide](#). The rapid development of technology, especially AI, has put social media platforms in the spotlight, as they will play a crucial role in political campaigns and, thus, the result of the elections. This month has witnessed a notable surge in proactive measures on social media platforms, launching campaigns to combat the spread of misinformation and safeguard democratic election processes.

National legislation

To begin with, Hawaii's (USA) new [H.B. 5141 \(S-1\)](#) bill on AI and political campaigns would require political advertisements generated in whole or substantially with the use of AI by a candidate or committee to include a statement that the advertisement is AI-generated. In their brief, officials stated that such measures are crucial because 'political campaigns have already used AI, and some believe that the proliferation of AI-generated images and other media could be used to misinform voters and interfere with elections.'

The role of intermediaries

[A coalition of 20 major tech companies](#), including OpenAI, Microsoft, Adobe, TikTok, and X, has declared a joint initiative to combat deceptive AI content potentially threatening global elections this year. Unveiled during the Munich Security Conference, the effort addresses concerns over the rapid proliferation of generative AI, which is proficient in swiftly generating text, images, and video in response to prompts. The accord outlines commitments to collaborative endeavours, including developing tools for content identification, public awareness campaigns, and measures against inappropriate content on their platforms. Potential technologies explored include watermarking or embedding metadata to certify the origin of AI-generated content.

EU elections

TikTok will launch an Election Centre within its app, tailored to EU member states' languages, [to combat misinformation ahead of the upcoming election year](#). TikTok aims to detect and remove misinformation and covert influence campaigns by collaborating with local electoral commissions, civil society groups, and nine fact-checking organisations. Additionally, the company aims to recognise and identify misleading AI-generated content (AIGC) by requiring content creators to label any realistic AIGC.

In addition, Meta stated that it will establish [a team to tackle the spread of disinformation and the misuse of generative AI](#) in the lead-up to the European Parliament elections scheduled for June 2024. Namely, Meta's Head of EU Affairs, Marco Pancini, announced plans to establish an Elections Operations Centre tasked with identifying and addressing potential threats in real-time, as stated in a blog post.

Lastly, Google announced that its Jigsaw Unit, dedicated to addressing societal threats, is set to [launch a campaign across TikTok and YouTube in five EU countries](#), including Belgium, France, Germany, Italy, and Poland, ahead of EU elections. Expanding on past campaigns in Germany and central Europe, Jigsaw is launching a new project where ads employ prebunking techniques developed with researchers from the Universities of Cambridge and Bristol, helping viewers recognise manipulative content before exposure.



Germany's new digital foreign policy strategy: Between continuity and change

Germany has joined Denmark, Switzerland, Australia, and a few other countries in outlining its [digital foreign policy in a strategic document](#). The strategy revolves around three pillars: safeguarding human rights in the digital realm, fostering prosperity in the globalised digital economy, and ensuring sustainability and resilience in the digital society.

The focus on data emerges as a central theme, with Germany advocating for an international agreement on the free flow of data. The strategy emphasises security aspects of data governance, marking a shift from its previous emphasis on the interplay between trade and privacy. Additionally, there is a stronger emphasis on involving national data protection authorities in policy implementation. However, AI receives relatively low prominence in the strategy, mentioned briefly in two paragraphs, with potential reasons for this reduced visibility yet to be clarified.

A paradox about inclusion is highlighted, where the pressure to create new bodies for digital governance may hinder the meaningful participation of smaller actors and disadvantaged groups. The strategy urges a cautious approach, aligning with the Bauhaus principle of 'form follows function', suggesting that new mechanisms should only be established if current ones prove ineffective.

Surprisingly, the strategy lacks direct references to WTO e-commerce negotiations, raising questions about a potential shift away from such negotiations. Germany aims to increase its presence in international standardisation bodies, emphasising a shift from purely technical standards to considering fundamental rights in standardisation processes. The strategy acknowledges the tension between industrial and societal

digitalisation and calls for innovative approaches to inclusion in standardisation that reflect the priorities and capacities of smaller and developing countries.

The strategy emphasises the importance of geo-redundancy and avoiding critical dependencies on digital infrastructure, particularly submarine and terrestrial cables. While China is not explicitly mentioned, the strategy indirectly touches upon digital issues relevant to Germany-China relations, such as technology leakage and dual-use concerns.

Net neutrality, absent from policy focus for some time, makes a return in the German strategy. How it will be implemented practically remains to be seen.

The document concludes by outlining the challenges in implementing the strategy, including reconciling the tension between values and interests, addressing issues missing from the strategy, and navigating the complexities of industrial and citizen digitalisation.

A longer version of this text is [available on Diplo's blog roll](#).



About this issue: Issue 87 of the Digital Watch monthly newsletter, published on 5 March 2024 by the Geneva Internet Platform and DiploFoundation. For more coverage and analysis, visit the [Digital Watch observatory](#)

Team: Andrijana Gavrilović (author), Boris Begović (contributor), Anastasiya Kazakova (contributor), Bojana Kovač (contributor), Yung-Hsuan Wu (contributor), Ginger Paque (editor), Diplo's CreativeLab (design) | Get in touch: digitalwatch@diplomacy.edu

On the cover: *Agreement on UN cybercrime convention elusive*. Credit: Vladimir Veljasević DiploFoundation (2024) <https://creativecommons.org/licenses/by-nc-nd/4.0/>

The Geneva Internet Platform is an initiative of: