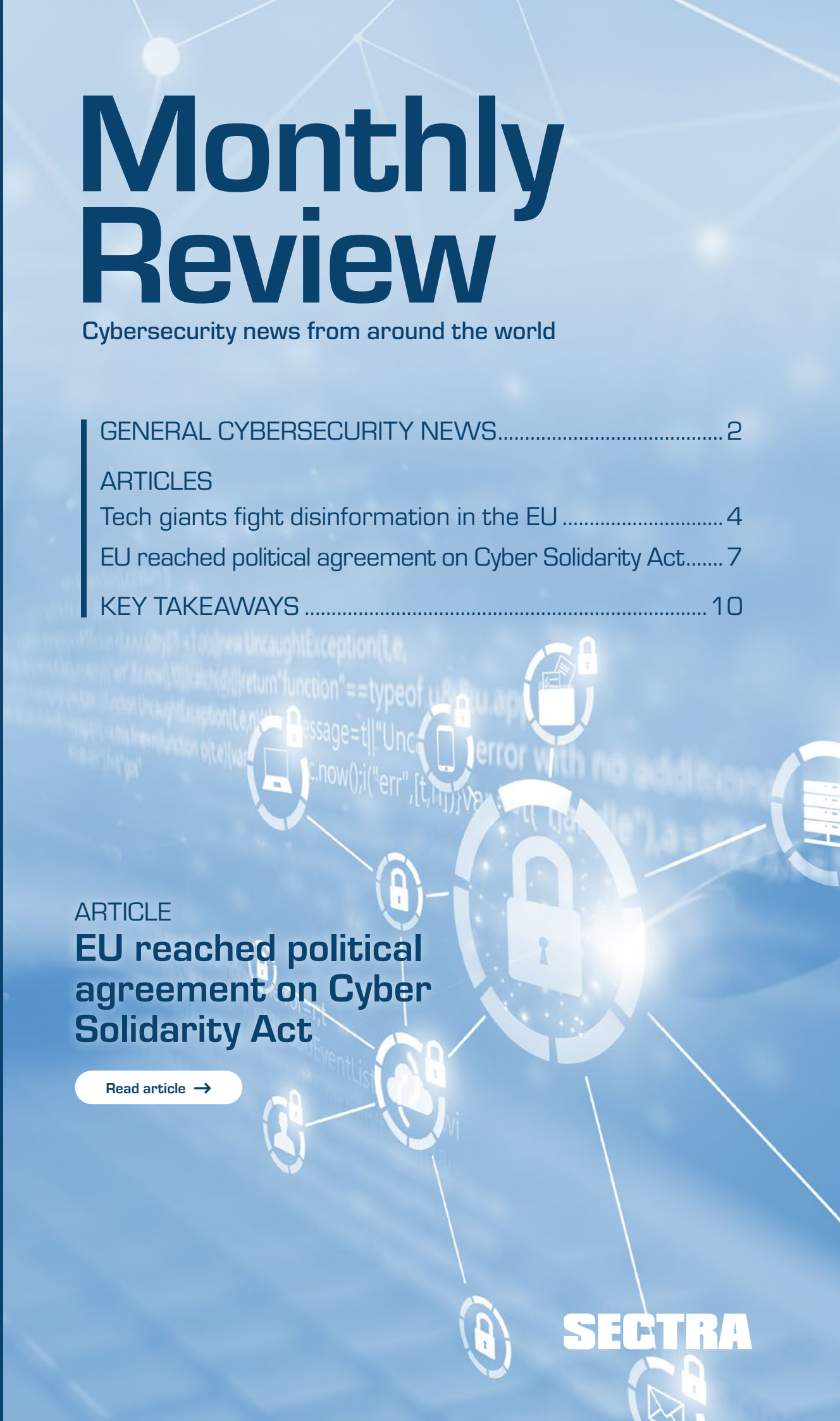
Monthly Review

Cybersecurity news from around the world



ARTICLE

EU reached political agreement on Cyber Solidarity Act

Read article →

SECTRA

General cybersecurity news

1 Browsing history data is valuable

The US Federal Trade Commission (FTC) has fined security company Avast $16.5 million for collecting and selling users' data without their knowledge or approval. Avast marketed its products as privacy and anti-tracking services, but in reality, its browser extensions and antivirus software collected users' browsing data. The collected data was sold for marketing and profiling purposes, violating both the law and the promises made to its users.

Browsing and search history reveals valuable information about users, including their age, gender, interests, and even religious and ideological orientation. Marketing companies compile this data to profile users for targeted marketing. Though preventing tracking is challenging, users can research a service provider's reputation and be cautious of using cheaper products that may profit through alternative means. It's important to remember that browsing data is also collected by malicious parties who may use it for crimes, such as pressure or blackmail.

2 New perspective on Chinese cyber influencing

Chinese cybersecurity company I-Soon suffered a data leak in February that revealed the Chinese government was soliciting bids for cyber espionage and hacker assignments with private service providers. The leak shows that I-Soon operates as a private cyber espionage contractor for Chinese security authorities and has developed its own malware. The leak changes the perception of Chinese cyber espionage activities, as it reveals that private cyber companies can also be behind the attacks. There is competition between service providers that may impact the effectiveness of future cyber operations. Organizations with ties to China should take this change into account.

3 Successful information management helps in cyber incidents

The importance of information management is emphasized especially in the event of the worst, i.e. when an organization is the victim of a cyberattack, and when investigation on what information the threat actor may have gained access to is ongoing. If, due to inadequate information management, an organization cannot respond quickly enough to whether sensitive information related to customers or partners has ended up in external hands, it is not likely to strengthen the trust of these parties in the organization. At worst, it may lead to accusations that the damage caused by the attack is being covered. It is necessary to have accurate information about where and how data is stored, as this can determine what information may have ended up in the hands of a threat actor. Compliance with guidelines must be adequately monitored through audits, and it must be ensured that instructions are implemented in practice. Furthermore, employees should not be put in situations where the performance of work and information management instructions conflict.

ARTICLE

Tech giants fight disinformation in the EU

The anti-disinformation front in Europe received new reinforcements in February when Google and Meta announced that they would launch campaigns to combat disinformation in the context of the European parliament elections in June. In particular, the EU has feared an increase in Russian propaganda and its impact on the upcoming elections.

The companies announced their plans around the same time the European Union's Digital Services Act (DSA) came into effect on February 17th. The DSA is meant to help fight disinformation by imposing obligations on online platforms, including on platform moderation, and by obliging platforms to assess and mitigate risks related to democratic and electoral processes. The DSA has already applied to large online platforms and search engines since August 25th.

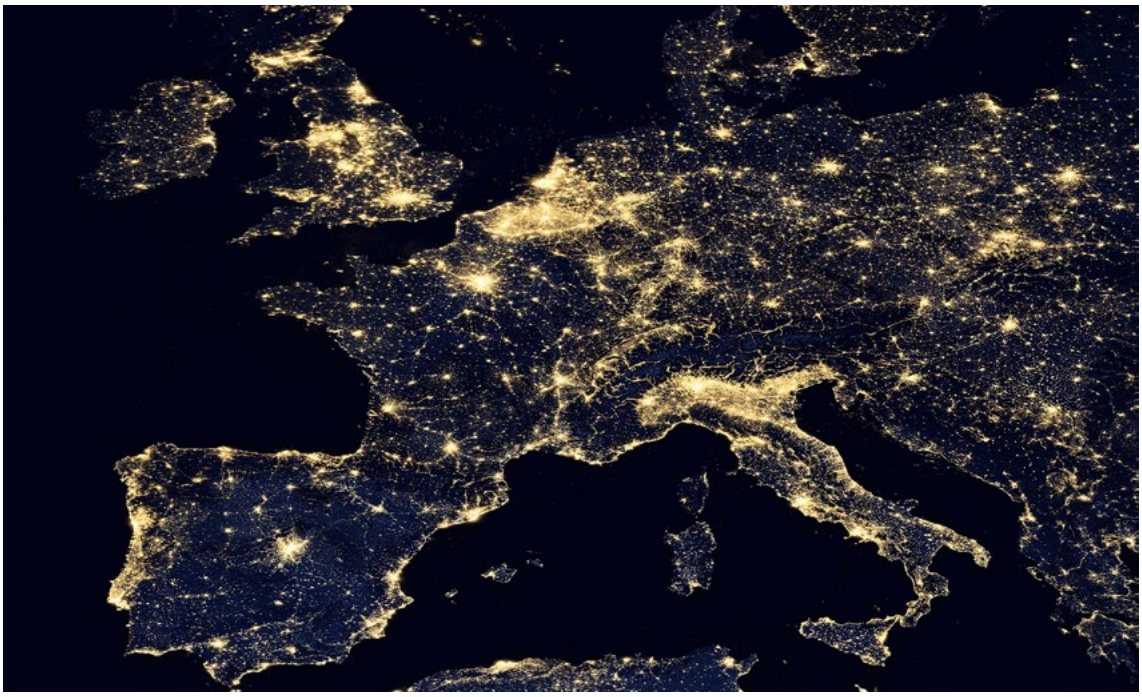
In Google's case, the company will launch an advertising campaign between April and May in different platforms, including YouTube and TikTok, in five EU countries: Belgium, France, Germany, Italy and Poland. The advertisements contain information on how to identify misinformation and disinformation and what kind of misinformation is sought to spread. The campaign uses so-called "prebunking" methodology. This means that the aim is to get the target notified of false information earlier than the false information itself reaches the target. When such misinformation reaches the target, he already knows to take it with caution. →

The countries were chosen for advertising to reach a large number of voters in the elections and to make use of the company's own local knowledge. The advertising campaign only targets the EU's most populous countries, which means many eligible citizens from other member states are left out and makes it less effective. Despite this, the measures taken are a step in the right direction.

Meta, meanwhile, is addressing the problem by opening a dedicated Elections Operation Center to identify and counter threats in real time. Tackling misinformation includes fact-checking with 26 partners across the EU in more than 22 languages. In addition, the aim is to tackle coordinated influencing operations and respond to possible misconduct with artificial intelligence, such as deepfakes.

"The aim is to increase users' rights and influencing opportunities."

Both companies' decisions are certainly partly influenced by the EU's Digital Services Act, although the announcements do not directly refer to it. According to the European Commission, the main objective of the act is to prevent illegal and harmful activities online and combat the spread of disinformation. However, the DSA has so far received more public attention for its obligations to allow platform users to opt out of personalized marketing, the obligation to create easily understandable terms of use, the obligation to moderate content more openly and the possibility to appeal against the moderation decision. In addition, the DSA unequivocally prohibits targeting advertising at children and targeting advertising at adults on the basis of, for example, ethnic background or sexual orientation. The aim is therefore to increase users' rights and influencing opportunities. →



Although the act itself applies to virtually all digital services, it focuses on very large online platforms and search engines. By definition, this includes services whose monthly number of active users exceeds 45 million users in the EU area when examining the average for a six-month period. For these very large operators, an additional obligation is to assess four distinct risk categories, for which measures should also be taken to reduce risks. These include risks related to the dissemination of illegal content, such as the spread of illegal hate speech, democratic processes, civil dialogue and electoral processes. The maximum number of fines for non-compliance with regulatory obligations can be up to 6% of a company's annual worldwide turnover.

EU regulation is often described as bureaucratic and its achievements are doubted. However, it is clear that it also has positive effects. DSA is possibly an example of successful regulation from the citizen's point of view, as it increases the transparency of services and users' choices regarding their own privacy. For wider society, campaigns resulting from this regulation can also reduce the effectiveness of attempts to influence the EU by hostile actors. ■

ARTICLE

EU reached political agreement on Cyber Solidarity Act

The European Union is stepping up cybersecurity regulation with yet another act. The Commission's April 2023 initiative for the Cyber Solidarity Act (CSA) received political approval last week in negotiations between the European Council and the European Parliament.

Next, the proposal for a regulation will proceed to formal adoption by the European Parliament and the Council, after which it will enter into force in accordance with the EU regulation process. Acts are binding and must be applied in full and directly in the EU member states. In other words, they differ significantly from directives, where Member States can decide for themselves how to achieve the goal set by the EU. What is the Cyber Solidarity Act about?

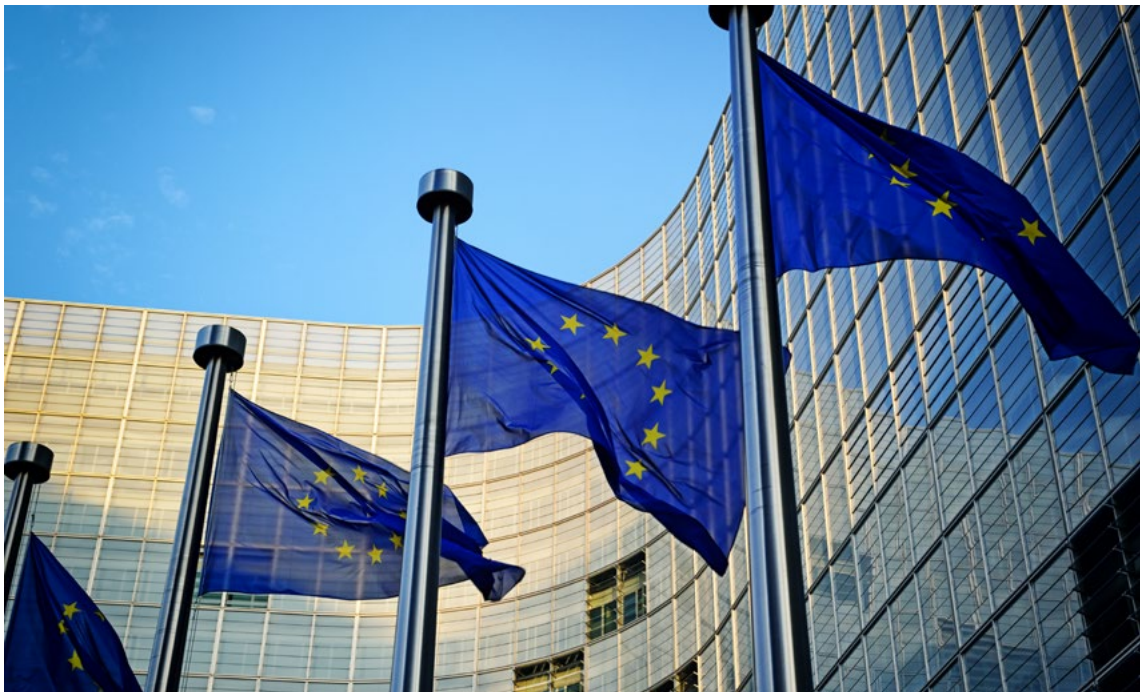
According to the European Commission, the regulation aims to improve the EU's cyber resilience. At the same time, it is hoped that it will promote solidarity between member states and the EU's ability to identify, prepare for and respond to cyber threats. In practice, the regulation introduces three new functions for the EU. The first is the European Cybersecurity Alert System. Its task is to detect cyber threats and provide real-time situational awareness to authorities and other relevant actors. The alert system would consist of a network of Security Operations Centers (SOCs) operated by member states to identify and disseminate threat information across borders. →

Secondly, the regulation establishes a Cybersecurity Emergency Mechanism to improve the ability to respond to major and large-scale cyber incidents. The mechanism consists of three components: preparedness actions in critical sectors, the establishment of a so-called "cybersecurity reserve" and financial support from member states to a state affected by a major or large-scale cyber incident.

Thirdly, the regulation establishes a European Cybersecurity Incident Review Mechanism, which should review and assess cybersecurity incidents and make recommendations based on that to improve cybersecurity in the EU. The European Union Agency for Cybersecurity (ENISA) would play an important role in this, producing a report on what lessons can be learned from the event and what recommendations can be made.

"Although the act seems to be more aimed at nation states, it also includes elements concerning private companies."

Although the act seems to be more aimed at nation states, it also includes elements concerning private companies. This is the case, for example, with the above-mentioned idea of a "cybersecurity reserve", where private sector "trusted actors" would be ready to act at the request of a Member State, an EU institution, agency or a partner non-EU country in the event of a large-scale cybersecurity incident. In addition, the preparedness actions mentioned in the emergency mechanism include coordinated testing of the preparedness of entities operating in highly critical sectors. →



The regulation follows other pieces of EU legislation dealing with cybersecurity, such as the NIS2 cybersecurity directive and the Cyber Resilience Act, the latter of which aims to ensure the cybersecurity of digital and related products. For the time being, it is difficult to assess the effectiveness of the Cyber Solidarity Act — the underlying idea of cooperation, solidarity, sharing threat awareness and learning from mistakes is, of course, to be supported. Much will depend on practical implementation and on how cooperation can actually be made to work.

From a critical point of view, the option in the emergency mechanism of financial support for a member state in distress is to be noted. One fear may be that the regulation will become one of the means of transferring funds within the Union, where member states that handle their cybersecurity well will have to pay for the mistakes or indifference of the less well-managed member states. This aspect has not been the subject of much debate so far, but as the level of cybersecurity varies widely across member states and as economic issues remain a sensitive political topic within the Union, it is also worth noting. ■

Key takeaways

1. The user's browsing history data is of interest to many different actors. In addition to criminals, marketing companies also seek this data.

2. Leaked information reveals private companies can participate in state-sponsored cyber espionage, changing the perception of China's activities.

3. Proper information management is crucial to avoid failures and ensure cybersecurity.

4. Google and Meta announced measures to combat disinformation ahead of June's European parliament elections.

5. The Cyber Solidarity Act aims to improve the EU's cyber resilience and cooperation between Member States. It is a continuation of other EU cyber regulation, such as the NIS2 Directive and the Cyber Resilience Act.

communications.sectra.com
communications@sectra.com

Sectra Communications is headquartered in Linköping, Sweden, and operates through offices in Sweden, the Netherlands and Finland.

SECTRA