Cyberwatch Finland

WEEKLY REVIEW
WEEK 4/2024

”CYBERSECURITY IS BUILT BY SMALL ACTIONS AND MANAGEMENT OF LARGE CONCEPTS”

Cyberwatch Finland

KEY TAKEAWAYS

1. The World Economic Forum (WEF) has taken a prominent stand on cybersecurity. Future threats include unwanted election interference and artificial intelligence.

2. The Airdrop app has been popular in China, especially in opposition activities. Now, the state claims to have gained access to the app's encrypted data.

3. Securitization is used to justify exceptional political measures. Cybersecuritization can also serve as a reason for example for increasing online surveillance

1. WORLD ECONOMIC FORUM AT THE HEART OF CYBERSECURITY

The World Economic Forum (WEF) has recently profiled itself as a vocal advocate for cybersecurity. On January 10, the Foundation published its Global Risk Report for 2024, which brings together leading insights from more than 1,200 experts around the world on short- and long-term risks. According to the report, cyber threats are among the top ten threats by experts in both timeframes. A day later, the WEF released a report looking at the 2024 outlook for cybersecurity. Cybersecurity also featured prominently at the Foundation's 54th annual meeting, which was again held in Davos, Switzerland on 15-19 January. In addition to having dedicated panels to the theme, including future scenarios for cyber security and tools for cyberdefenders, it was touched upon in several other speeches.

In order to understand the significance of WEF, its reports and the annual meeting, it is important to consider the background of the organization. The World Economic Forum is a foundation funded by large transnational corporations to promote globalisation, free trade and public-private partnerships. The Annual Meeting, in particular, is an important discussion platform for topical issues. In Davos, business leaders and politicians meet every year. Finland was represented at the event by Minister for Foreign Affairs Elina Valtonen and Minister of the Climate and the Environment Kai Mykkänen. The value of WEF lies in its think-tank-like and unifying nature, where space is created for different ideas, expert speeches and futures thinking.

Of the cybersecurity considerations highlighted in WEF's reports and panel discussions at the event, the most fruitful is to examine future threat scenarios and the solutions offered for them. For example, Ann Cleveland, executive director of the Center for Long Term Cybersecurity at the University of California, Berkeley, highlighted four looming future scenarios for cybersecurity. These include disruptions in microchip production and global production chains, constantly evolving deepfake materials and election interference, DNA data ending up in the wrong hands, and artificial intelligence. According to Cleveland, when responding to problems, it would be necessary to remember the principles of security by design in new applications. Also training and cybersecurity awareness play a significant role in responding to threats. Cleveland also pointed out that the future doesn't necessarily have to look negative. For example, labour productivity may increase as a result of robotisation and new technology, and active cyber cooperation could be used to tackle crime better than before.

Although Cleveland also sought a positive approach in its introduction, the statistics and other speeches at the event indicate that the threat landscape is becoming more diverse, and the future looks rather bleak. For example, in a panel discussion on the possibilities of cyberdefenders, an Interpol representative said that the situation is challenging, because the more cybercrimes are investigated, the more they are uncovered. When investigating a single cybercrime, many more are often revealed in the same case. Also, the increasingly digitalised world increases the threat area to a significantly larger size. Increasing geopolitical tensions add their own spice to the mix. More than 70% of the respondents to the background material for WEF's cybersecurity outlook report say that the geopolitical situation has affected company's cyber security. In addition, less than one in ten respondents believe that AI will work to the benefit of cyberdefenders.

Looking at the WEF data, it is obvious that cyber security is no longer a matter of its own in a vacuum. Cyber security has become an issue that has expanded to every area of life and is a key part of society's overall security and future solutions. The annual meeting discussed, among other things, climate change adaptation applications, biotechnology and the war in Ukraine. In all of these, there was also a place for the cyber element. From the perspective of ordinary citizens and organisations, the future can best be influenced by anticipating, preparing for and maintaining current cyber threat awareness. That way, even unpredictable events and future developments will not come as complete surprises.

2. CHINA CLAIMS TO HAVE CRACKED APPLE´S DATA TRANSFER APP, WHICH IS POPULAR WITH THE OPPOSITION

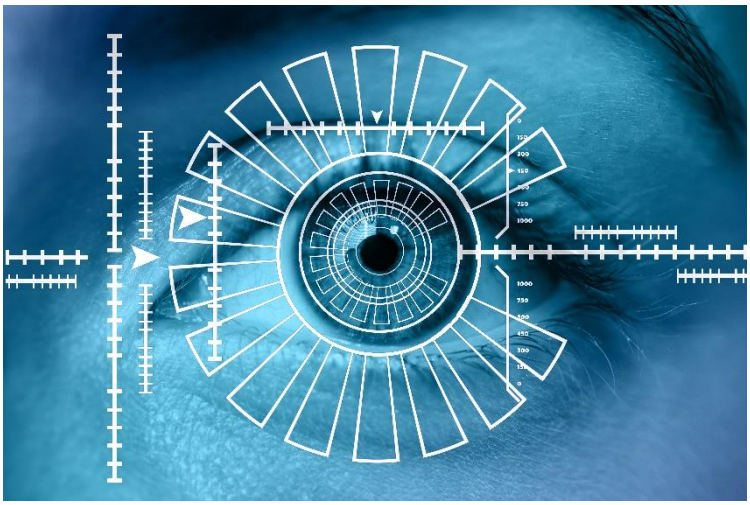
A Chinese research institute claims to have successfully cracked Apple's secure device log and thereby also obtained log data from Apple's Airdrop data transfer app. This information includes phone numbers, email addresses, and device names whom the hacked device has been in contact with. In order to open these logs, the researchers needed to gain physical access to the device on which the data had been shared. German researchers say they discovered the vulnerability now being exploited by the Chinese back in 2019 and reported it to Apple. However, it seems that Apple has not taken the necessary corrective measures to make the operating logic of the application more secure.

As such, the method used by the Chinese is not suitable for mass surveillance, for example, but enables log data retrieval from retrieved devices. The use of the Airdrop app has been particularly popular in connection with the protests in China, as it has been impossible to trace and monitor until now. The app does not use the internet or require a mobile network connection, because data transfer takes place locally via Bluetooth and a private Wi-Fi network. In practice, the application can be used to share a message or share files with nearby devices, without prior contact with the receiving or sending device, or contacts. This has enabled communication and information sharing also in situations where the Chinese state has sought to make it more difficult to organise and organise opposition activities, for example by turning off the mobile network during protests. However, disconnecting the mobile network has not affected the use of the Airdrop app in any way, so it has been a very valuable tool for activists. For example, the app was a very popular information-sharing platform during the 2019 Hong Kong protests. After the 2022 protests, China demanded that Apple limit the app's functionality, to which Apple agreed. The change first took effect in China and later globally. After the change, the app will only be able to share files between devices in the device's contacts, or for a limited period of 10 minutes, also between other devices.

With an annual market share of about 15% of mobile phones sold in China, Apple has been a major player in the market. About 20% of Apple's total sales come from the Chinese market, so the Chinese market has been particularly important and profitable for it as well. This probably explains why Apple agreed to reduce the functionality of the Airdrop app at China's request. The case that has now come to light may also bring tensions between China and Apple. China's big exit with the Airdop crack seems to be aimed primarily at users of Apple and other Western technology in China. The aim is probably also to raise the threshold for using the application in opposition activities, because even though the technology does not enable mass surveillance, the risk of being tracked and identified through it may reduce the attractiveness of use. In this way, China is showing that it maintains control over these technologies as well. China has also banned government agencies from using Apple devices in their work or even bringing Apple devices to workplaces.

3. CYBERSECURITIZATION AS A POLITICAL TOOL

Securitization theory is a theory developed by Danish political scientist Ole Wæver that has gained visibility also in public debate. In securitization, something is transferred from the area of normal politics to a separate domain of security. Preventing an event or issue defined as a security threat may require extreme measures that are by nature authoritarian, coercive and potentially undemocratic. Security threats often also have a unifying effect on the people. It may therefore be tempting for politicians to present an issue as a security threat. That way one could justify actions that would be excluded in a normal democratic society and, and at the same time, present oneself as a decisive and strong leader. There are indications that cybersecurity has also started to be a part of securitization. Cybersecurity threats are used to justify increased control and supervision and bans on the use of applications, among other things.



Cybersecuritization has been most visible in authoritarian countries. Turkey, for example, has long controlled its citizens' online use. Correspondingly, attempts have been made to circumvent surveillance, for example, with VPN applications. As the latest information, practically all major VPN operators used in the country have been banned by the state. The official reasons given are to reduce foreign influence and ensure national security, but in reality, the aim is probably to increase control and, for example, make it more difficult to monitor alternative media. Blocking VPN operators is already familiar from countries such as China and Russia. Often, however, new VPN operators become available to consumers very soon, which those in power have not yet had time to block. Full censorship in the case of Turkey is unlikely to be achieved either, but the ban will cause extra inconvenience to knowledge-hungry citizens, reduce their opportunities and raise the threshold for access to alternative information.

Securitization can also be done in Western countries and free democracies. In France, for example, the government has switched to the French messaging app Olvid because "popular" apps have allegedly posed a security threat. Although the applications were not specified, it is likely that the comment refers to apps such as WhatsApp and Signal, which are generally considered reliable apps. Most likely, the intention is to favour the French application and increase its popularity. Some similarity can also be seen in the heated TikTok debate, where the security of the Chinese app has been doubted and it has even been raised as a national security threat in many countries. There has been discussion about a possible ban on the application, for example in the United States. However, conclusive evidence that TikTok is dangerous has not been presented.

The key question in securitization, especially in Western countries, is how to balance democracy, freedom and prohibitions and, for example, the supervision of security authorities. Although there may be legitimate risks behind security concerns, one should not shoot a fly with a cannon. In the case of TikTok, for example, one should consider whether it is necessary to ban the app altogether, as this could open Pandora's box for subsequent bans that might not be as justified. The father of the securitization theory, Ole Wæverin, has suggested that each sector should be treated on its own terms. Climate issues would be dealt with as climate issues, religious issues as religious issues. Perhaps cybersecurity should also be dealt with in its own field of cybersecurity. This does not mean that cyber threats should not be taken seriously, quite the opposite: the importance of organisation-specific risk analyses is emphasised as part of management's growing role in the comprehensive management of cybersecurity. Cyber risks can have significant consequences for societies and individual organisations. However, when deciding on measures, patience is key, and not all action should be sacrificed on the altar of safety. Instead of prohibition, the means could be to develop citizens' cybersecurity skills and raise risk awareness to increase secure behaviour. At the same time, raising awareness of the value of the user's own data and its significance could serve as a means of combating applications suspected of espionage.

REFERENCES

1. World Economic Forum at the Heart of Cybersecurity

https://www.weforum.org/events/world-economic-forum-annual-meeting-2024/
https://www.weforum.org/publications/global-risks-report-2024/
https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

2. China Claims to Have Cracked Apple´s Data Transfer App, Which is Popular With the Opposition

https://www.techtarget.com/searchsecurity/news/366565895/China-claims-it-cracked-Apples-AirDrop-can-track-senders
https://sfj.beijing.gov.cn/sfj/sfdt/ywdt82/flfw93/436331732/index.html
hthttps://www.bleepingcomputer.com/news/security/china-claims-it-cracked-apples-airdrop-to-find-numbers-email-addresses/#google_vignette
tps://www.counterpointresearch.com/insights/china-smartphone-sales-q3-2023/
https://edition.cnn.com/2024/01/12/tech/china-apple-airdrop-user-encryption-vulnerability-hnk-intl/index.html
https://www.statista.com/chart/13246/apple-china-revenue/
https://www.cbsnews.com/news/china-apple-airdrop-encryption-cracked-to-block-inappropriate-information/

3. Cybersecuritization as a Political Tool

https://cybernews.com/news/turkey-vpn-ban-elections/
https://www.lemonde.fr/en/economy/article/2023/12/15/olvid-the-french-government-s-secure-messaging-app-already-under-fire_6346249_19.html
https://www.politico.com/news/2023/04/16/why-washington-wont-ban-tiktok-00091690
https://www.helsinki.fi/fi/uutiset/politiikka/turvallistamisen-teorian-avulla-voidaan-tutkia-turvallisuusuhkia-sodista-ilmastonmuutokseen
Columba, Peoples, Vaughan-Williams, Nick. 2014: Critical Security Studies: An Introduction, 2nd edition. Abingdon. Routledge 2014.

Pictures: Pixabay