WORK AND DIGITALISATION 20.07.2021 | Ekaterina Venkina

How Denmark became the most cyber-secure country

In a world where countries worldwide are facing increasingly sophisticated cyberattacks, Denmark is leading the global race in cybersecurity

'Don't open this e-mail from "McDonald's".' The word 'Warnings,' white against the green background, screams at me from the top of the mobile phone display. Below it, 'Vi er kede,' Danish for 'We are sorry,' is accompanied by a yellow letter M. It looks as familiar as can be, and automatically makes you think of greasy burgers and fries, a guilty pleasure on late office work days.

The notification is an alert about a fraudulent e-mail circulating disguised as a message from McDonald's. The warning was sent by the Danish app 'Mit digitale selvforsvar' ('My digital self-protection'). According to the head of the project, Ulla Malling, the application 'has already been downloaded 250,000 times since its launch in April 2017 and has an average of 80,000 active users per month.'

The app provides information about digital scams, threats from viruses and malware, live updates from banks and law enforcement authorities, and even gives concrete advice if a breach has occurred. The initiative is a result of a collaboration between The Danish Consumer Council (Forbrugerrådet Tænk), a non-profit entity TrygFonden, the financial sector and The Danish Crime Prevention Council (Det Kriminalpræventive råd).

More importantly, however, the app is the epitome of the Danish approach to cyber and information security with its near-perfect synergy of different institutions and focus on the everyday safety of citizens and businesses.

Denmark: Primus inter pares

Until recently, the country with a population of just over 5,8 million was

clearly overshadowed in the public eye by cybersecurity big league players like the United States, Israel and the United Kingdom. But now it seems to have finally gained enough momentum to step into the spotlight.

Over the next few years, Denmark plans to invest at least DKK (Danish kroner) 1.5bn (€202 million) in its cyber and information security.

This year, the Ministry of Foreign Affairs announced that Denmark ranked first among the world's most cybersecure countries with an average overall score of 3.56, according to the British security research firm Comparitech. How did Denmark achieve that? And did it have to do with the country mobilising its information security efforts after a major security breach in 2015-2016 that Copenhagen linked to 'the intelligence services or central elements in the Russian government'?

'A very critical situation'

In April 2017, the Copenhagen newspaper Berlingske published some of the conclusions from the report by the Danish Defence Intelligence Service's Center for Cyber Security (CFCS). It revealed that the same hacking group behind a 2016 cyberattack on the US Democratic Party servers had gained access to 'the e-mail accounts of select members of the Danish Defence.' Even though the leaked data was described as non-classified, it could still be used 'to blackmail staff into becoming agents,' CFCS said.

Denmark's then defence minister, Claus Hjort Frederiksen, rated the breach as a 'very critical situation.' According to several intelligence agencies, the group behind the attack was most likely APT28, also known as Fancy Bear, which is widely associated with Russian military intelligence.

Now, only four years after the attack came to light, Denmark tops Comparitech's ranking as the world's most 'cyber safe' nation. According to Rebecca Moody, the lead researcher, Denmark was placed in the top three ten times out of a possible 15. It had zero users attacked by mobile ransomware trojans and mobile banking trojans. It also scored particularly well in categories such as percentage of users attacked by ransomware trojans (0.02 per cent) and percentage of attacks by cryptominers (0.11 per cent).

Although the study, based on Kaspersky Lab's Q3 2020 data, is largely malware-centric and does not offer deeper insights into legal and strategic

issues (in the Global Cybersecurity Index 2018, which does, Denmark ranks 12th in Europe region with a score of 0,85), it does give an indication of what the Danes are particularly good at: individual digital hygiene and financial services security.

The latter is at least partly due to the widespread implementation of two-factor authentication. It successfully helps block certain attack vectors, considering that personal digital signatures are used as a login for all governmental online services and in the financial sector. Another game changer is well-developed banking apps.

A wake-up call

Over the next few years, Denmark plans to invest at least DKK (Danish kroner) 1.5bn (€202 million) in its cyber and information security. According to the government's strategy for 2018-2021, its policy is based on a triad: increasing technological resilience, improving citizens' knowledge and strengthening coordination between different actors. The country is now actively working on defining its critical infrastructure. This will help the government adopt emergency preparedness guidelines and breach prevention strategies.

So, do these efforts mean that Denmark has done its homework well after the major security incidents of 2015-2016? While Comparitech's study editor Paul Bischoff says: 'It sounds like it could be, definitely,' Rebecca Moody takes a more cautious stance: 'Probably. I think any time someone suffers a successful cyberattack, they're inclined to upgrade both their operational security and their cybersecurity.'

Even as 'the Russian hackers' continue to be perceived as 'les Enfants terribles' by the Western digital world, Moscow's stance on such groups remains ambiguous.

Lars Bajlum Holmgaard Christensen, executive director at the Danish Hub for Cybersecurity, recalls how security breaches were perceived by businesses when information about them first became public. 'I think it was a wake-up call for many companies. Awareness of the threats has increased after these attacks,' he says.

A 24/7 Situation Centre has been established at the CFCS to help maintain a national cyber situational awareness map. Also, 25 specific initiatives have been outlined to consolidate defences against cyberattacks, information technology criminals and external threats.

Since the data leak came as a serious warning, it is not too far-fetched to

assume that the Danish intelligence services' response to it must have been much more systematic and thorough than a simple 'let's patch it up' approach.

Moreover, Denmark's example as one of the NATO countries has certainly shown how fragile the technical balance has become in a world where Big Data multiplied by AI capabilities offer a new understanding of digital vulnerabilities amid increasing attacks by malicious cyber actors.

Moscow's ambiguous stance

Even as 'the Russian hackers' continue to be perceived as 'les Enfants terribles' by the Western digital world, Moscow's stance on such groups remains ambiguous. On the one hand, the Kremlin categorically denies that official Russian structures are involved in such attacks. On the other hand, there is a certain pride among the authorities, backed by official propaganda, in what Russian IT-geeks are supposedly capable of.

Nevertheless, according to Alexander Isavnin, a Russian Internet expert and lecturer at Free Moscow University, 'we can't really speak of a particular aversion of 'Russian hackers' to Denmark.' Rather, their modus operandi is to attack a series of vulnerabilities one after the other (often in different countries) in order to break through several 'security doors' in succession. The most widely used version of the internet protocol, IPv4 (as opposed to its next-generation successor IPv6), allows almost the entire internet to be scanned for vulnerabilities within minutes, thanks to a limited number of IP addresses and current network speeds.

As long as this status quo persists, Denmark will certainly continue to engage in cybersecurity, including in ways that look quite innovative to the rest of the world.

Moreover, the actors behind such attacks can be very diverse, he admits, be they 'scientific military units, outsourcers through various tech platforms, operators of hired malware, schoolkids or modern IT-equivalents of Soviet sharashkas,' research labs in the Gulag camp system. Their operational goal in most cases is, if not fishing for classified and hard-to-access information, then causing chaos. The lack of globally agreed procedures for dealing with cyber actors currently makes these forays possible.

What's next? Cyberdesign!

With all these developments, however, one important factor should not be forgotten, as it certainly contributes to Denmark's top position in Comparitech's world ranking. Unlike the US, Denmark is not currently perceived as a high-profile cyber target.

Although, as the June 2021 CFCS assessment shows, the threat level in terms of cyber espionage and cybercrime is very high, the threat of destructive cyberattacks on Danish authorities and private companies remains low. This means that in the eyes of the Danish intelligence services, it is very unlikely that something similar to the targeted ransomware attack on the US Colonial Pipeline will happen in the country anytime soon.

As long as this status quo persists, Denmark will certainly continue to engage in cybersecurity, including in ways that look quite innovative to the rest of the world. As part of its international efforts, it will further promote its cyber diplomacy. In 2017, the world's first 'techplomat' was appointed to strengthen the country's interests in Silicon Valley. The position is currently held by tech ambassador Anne Marie Engtoft Larsen, who replaced 'pioneer' Casper Klynge.

Another field with emerging potential is the coupling of various cybersecurity solutions with Danish innovative design, offering them as part of the package already at the product sketch stage. As the discourse around this new market thinking gains strength, the national business community seems increasingly inclined to see cybersecurity as their new growth adventure.

Ekaterina Venkina
Berlin

Ekaterina Venkina is a journalist focusing on politics and global affairs and an award-winning graduate of Columbia University's Graduate School of Journalism. She was a 2024 Post-Grad Pulitzer Center Reporting Fellow. During her decades-long career, she has lived,

studied, and worked in six different countries: Russia, Sweden, the United States, the United Kingdom, Belgium and Germany. She has been reporting for Germany's international broadcaster Deutsche Welle since 2014, most recently from Berlin.