Cyber threats in 2020 and beyond

Nordic strategic outlook

As the COVID-19 pandemic continues to trigger national and local restrictions across the Nordic region, the "new normal" appears to be here to stay. Businesses will need to adjust to a more permanently remote workforce and the challenges that entails – not least with regards to cyber security.

Beyond the pandemic, the threat landscape continues to be shaped by global events: from an increasingly confrontational struggle for technological supremacy between the US and China – one that is likely to continue to define our "new normal" for years to come – to emboldened cybercriminals weaponising the fear and disruption caused by the pandemic. Where does this leave the Nordic countries, and what are the key trends that will shape the cyber threat landscape in the region in the year to come?

Geopolitics drives increasingly fragmented cyber espionage threat, regulatory landscape as EU seeks strategic autonomy

The Nordic countries' geopolitical positions and innovative economies largely define the threat landscape for Nordic organisations, both at home and abroad. In 2020, we continued to see Russian and Chinese threat actors as posing the highest espionage threats to Nordic organisations: the former for strategic and political espionage – demonstrated most clearly in August's cyber attack on the Norwegian parliament – and the latter largely for commercial espionage, targeting sectors and technologies of strategic importance to domestic industrial policies and economic development.

Such state-linked advanced persistent threat groups (APTs) are likely to remain the primary threat to Nordic countries in 2021, though the espionage threat landscape in the region is becoming increasingly fragmented. In the past year, we have recorded espionage operations in Nordic countries by other capable actors, including groups based in Iran and North Korea, as well as emerging threat actors from states such as Turkey and India. Moreover, state actors' motivations are expanding beyond strategic and commercial espionage, as demonstrated by the targeting of Nordic countries for financial fraud and politically motivated disinformation and distributed denial of service attacks in the past two years (see Figure 1).

The intentions of state-sponsored threat actors towards individual Nordic countries and organisations will likely closely follow the broader strategic objectives of the state, both geopolitical and economic. National developments – including diplomatic tensions between Russia and Norway, and China and Sweden, and upcoming elections in 2021 (Norway) and 2022 (Sweden) – are also likely to affect the level of intent to target individual Nordic countries.

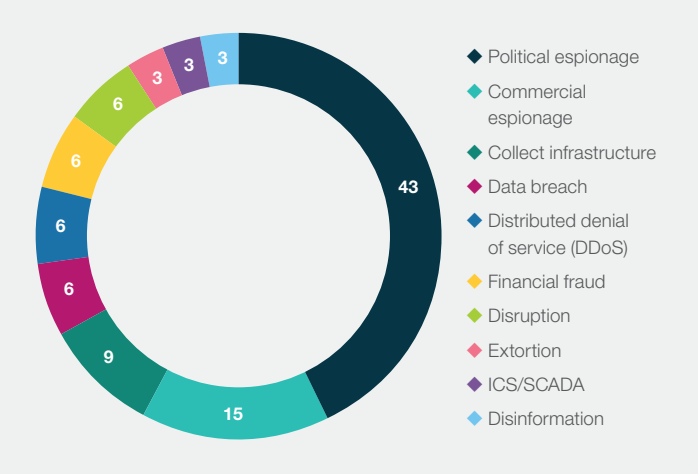
In addition, emerging geopolitical struggles between the US, China and Russia in the Arctic are likely to increasingly shape intelligence priorities as the region's resources become more accessible. This is driven both by strategic and commercial motivations, including the opening of new trade routes in the far north. The centrality of several Nordic countries in Arctic affairs and their high level of expertise in Arctic operations, including in the oil and gas and maritime sectors, likely make them attractive targets for espionage operations seeking to gain insight on Arctic policy positions, as well as technological solutions.

copenhagen@controlrisks.com controlrisks.com

Cyber threats in 2020 and beyond

Nordic strategic outlook

Fig 1 ▶ Targeting intent of significant state-sponsored attacks in the Nordic region, 2018–20 (%)



These broad, longer-term trends are likely to persist in 2021. Geopolitically driven cyber threats are likely to be most acute for government and public sector bodies, defence and national security agencies. However, state-sponsored targeting of Nordic countries also focuses heavily on critical sectors and infrastructure, including in the oil and gas and energy sectors, finance and telecommunications (see Figure 2). Private sector organisations operating critical national infrastructure will likely continue to face high threats from state actors such as Russia.

Meanwhile, technologies in sectors such as energy, maritime and oil and gas are also likely to remain a priority for state actors, particularly as more countries look to expand their domestic renewable energy sectors. Being at the forefront of renewable energy development and innovation, Nordic organisations are likely to be attractive targets.

More broadly, we also expect emerging regional developments in Europe to affect the cyber threat landscape for Nordic organisations in the coming year:

The EU draws the line

European governments and EU institutions are adopting a more assertive stance towards Russian cyber actions. In July, the EU for the first time used its new framework for cyber sanctions by imposing restrictive measures on Russian, Chinese and North Korean individuals and entities for their involvement in large-scale cyber attacks. In October, the EU further sanctioned several individuals linked to the Russian foreign intelligence service for the 2015 hacking of the German parliament.

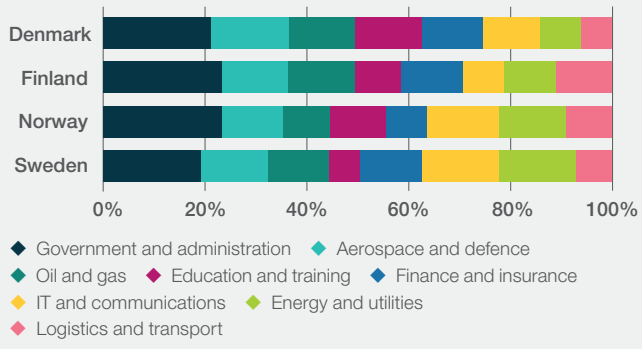
The Norwegian government's relatively swift attribution of August's attack on its parliament to Russia further attests to this trend. Precedent suggests, however, that these efforts are unlikely to significantly deter Russian cyber operations against European organisations; instead, they are likely to trigger a more assertive Russia, including in the cyber domain.

European strategic autonomy and digital fragmentation

Even before COVID-19, European leaders sought to define Europe's role in a global landscape increasingly shaped by the US-China trade war. The digital transformation triggered by COVID-19 has also brought a new sense of urgency to questions about the drawbacks of global interconnectedness. In the EU and across the Nordic region, questions are being asked about how reliant we are on foreign technology, solutions and services, and what this means for our national-level resilience and vulnerabilities.

These questions will continue to shape political and regulatory discussions as countries comes to terms with the "new normal". This is likely to further cloud the regulatory landscape for digital services and technology, particularly for businesses that operate across multiple competing – and sometimes conflicting – regulatory regimes.

Fig 2 ▶ Most targeted sectors in state-sponsored attacks in the Nordic region, 2018–20 (%)



copenhagen@controlrisks.com controlrisks.com

Cyber threats in 2020 and beyond

Nordic strategic outlook

Aggressive extortion threats pose new challenges to risk management

In 2020, large-scale and high-impact ransomware attacks became further cemented as a critical threat to organisations across countries and sectors. A multitude of operators with varying capabilities used new tactics, including widespread adoption of data leak extortion to pressure victims to pay. In October, data exfiltrated from a Swedish security company was released following a failed extortion attempt, when threat actors on the dark web leaked sensitive documents on the security measures of several of the company's high-profile clients. As we approach 2021, data leak extortion is firmly established as a tactic for dozens of ransomware operators, including some of 2020's most prolific cybercriminals.

Although extortive cybercrime is not new, the adoption of data leak extortion alongside encryption – or, in some cases, instead of it – means such attacks carry a wider set of risks for affected companies. Whereas ransomware extortion focuses on causing as much operational disruption as possible as a means to extort payments, data leak extortion focuses more on the reputational and regulatory impacts associated with breaches of sensitive information. Ransomware operators seek to create negative publicity and pressure from organisations' clients, customers, and other stakeholders to compel victims to pay.

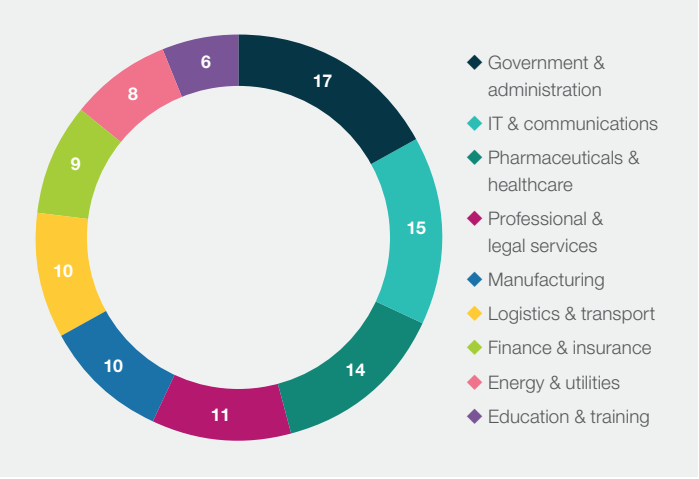
More broadly, ransomware operators are increasingly seeking to identify other areas of weakness in organisations that can be leveraged to extort a payment. We have seen ransomware operators set ransom demands below the likely level of a regulatory fine for the associated data breach, as an incentive for victims to pay. Conversely, companies need to consider the possible data breach implications associated with ransomware attacks upfront to ensure that legal and regulatory obligations, such as reporting requirements, are met. This is particularly the case for regulated entities with additional data security obligations. Further consequences of large-scale data breaches include civil lawsuits from victims and loss of business, as was the case following the disclosure of a major data leak extortion attack against a Finnish psychology clinic in October.

copenhagen@controlrisks.com controlrisks.com

Cyber threats in 2020 and beyond

Nordic strategic outlook

Fig 3 ▶ Most targeted sectors in ransomware attacks, 2018–20 (%)



We expect the threat of data leaks to remain a primary extortion tactic for cybercriminal operators, alongside ransomware attacks. At the same time, the ransomware threat landscape is likely to fragment with new malware strains and operators entering the space, with some focusing on the traditional operational impacts and others increasingly focusing on the reputational and regulatory angles to monetise their campaigns.

In 2020, we have also seen new and less experienced groups more swiftly adopt the tactics, techniques and procedures (TTPs) of established groups and co-operate with other groups to improve their capabilities. Such collaboration and exchange is likely designed to reduce competition – including the risk of targeting the same entities – as well as to complicate attribution and law enforcement action against specific operators.

The fragmentation of the threat landscape puts greater emphasis on understanding who is targeting you and what their objectives are, as this has a significant impact on risk management and response. In particular, the expanded use of sanctions against cyber threat actors by both the US and the EU means organisations may unwittingly engage with a sanctioned entity, which could lead to significant legal repercussions. Further, understanding your adversary's extortion tactics can help determine appropriate strategies during an attack.

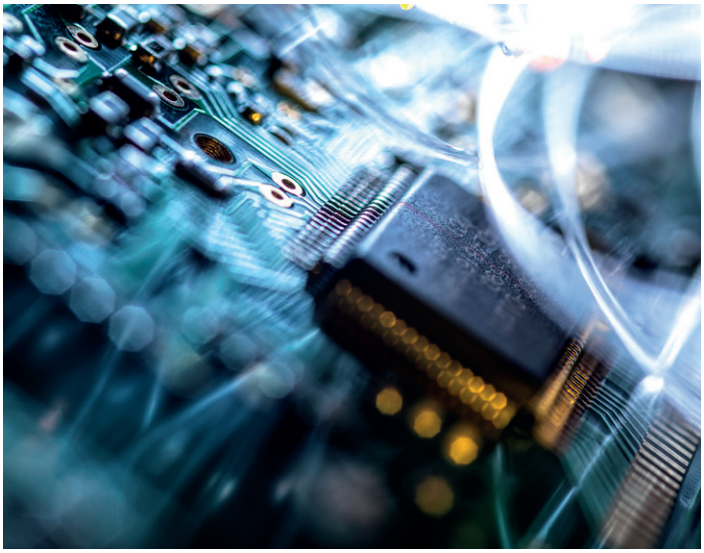
Large-scale, high-impact attacks are likely to become more frequent across the Nordic region and organisations will need to revise, reconsider and expand current risk mitigation and incident response plans accordingly. In particular, it is critical that organisations thoroughly prepare themselves for communicating with clients and other external stakeholders in the event of an incident, and ensure they know their regulatory obligations under for example the EU's General Data Protection Regulation (GDPR).

Environmental activists move online

Restrictions on physical gatherings have affected the cyber activist threat landscape. Even before COVID-19, we saw environmental activist groups such as Extinction Rebellion (XR) express intent to develop cyber capabilities and expand their campaigns in the digital domain, which has been followed by several online campaigns targeting the energy, oil and gas and financial sectors.

While cyber activism has typically been rare in the Nordic region, traditional environmental activist movements have a long track record of campaigns, and environmental issues are highly salient across the region. As such, it is hardly surprising that one of the first cyber tools deployed by XR was developed by a Danish cyber activist, and used to target several large Nordic organisations in the oil and gas, maritime and energy sectors.

While the tool itself was unsophisticated and the campaign had little tangible impact, the development indicates that environmentalist cyber activism is likely to pose a higher – albeit still relatively low – threat to Nordic organisations in the coming year. This is particularly the case for established targets for traditional environmentalist groups, such as companies operating or financing carbon-intense industries and projects. Such operations will likely continue to focus on relatively unsophisticated tactics and tools designed to create negative publicity, but we have also seen activists targeting senior executives, employees, shareholders and other key stakeholders to pressure companies.



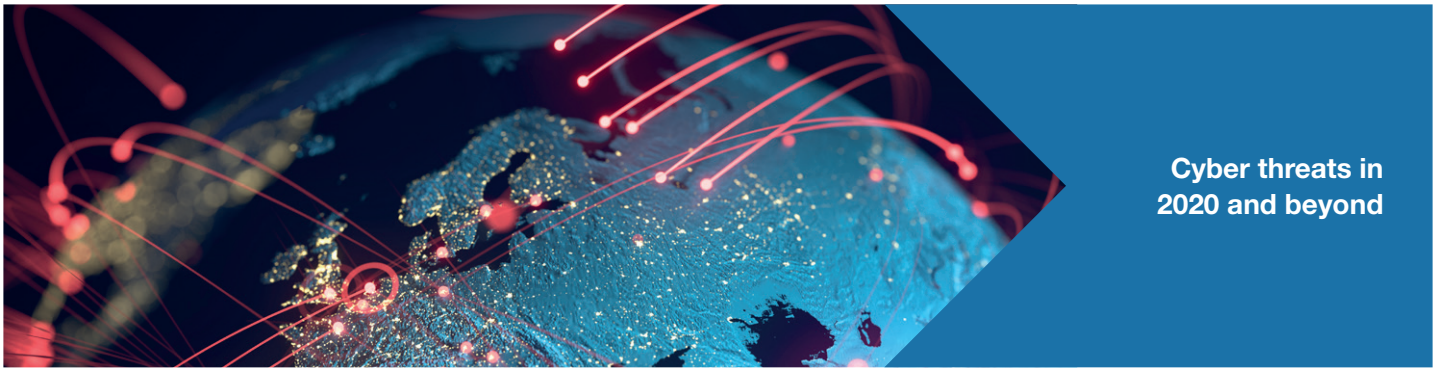
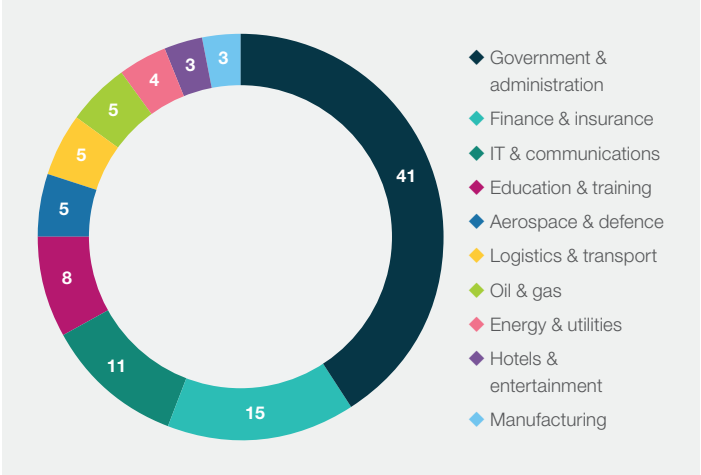


Fig 4 ▸ Most targeted sectors in cyber activist attacks, 2018–20 (%)



Increasingly sophisticated, fragmented disinformation space brings new threats to private sector organisations

The evolution of disinformation is likely to present growing threats to both public and private sector organisations in the coming years. State-backed disinformation campaigns are likely to remain a key trend in 2021. This is of particular importance for Norway and Sweden, which will hold elections in September 2021 and September 2022 respectively. Although direct interference in the elections is unlikely, foreign states, particularly Russia, are likely to use disinformation to fuel social and political divisions and erode trust in public institutions and electoral processes.

Other foreign states will likely also continue to pursue influence campaigns in the region in the coming year, seeking to shape public and political opinions on key issues including human rights and the treatment of minorities. Both state and non-state actors are also likely to intensify disinformation campaigns focused on COVID-19, as well as global vaccine efforts.

Beyond politically motivated campaigns, we are also seeing non-state actors adopt disinformation tactics for other purposes, using the ease of mass distribution online and increasingly refined toolsets, such as deepfakes enabled by artificial intelligence, to push their agendas. Through our client work we have identified a growing number of actors using disinformation tactics to target private companies, including on behalf of commercial competitors. In one case, a client was targeted through inauthentic online behaviour apparently orchestrated by a legitimate advertising company, with the aim of promoting a competitor's products.

Such examples show that we are a long way from the by-now relatively easy-to-spot Russian bots we are used to in the Nordic region. Given the fast pace of information and the difficulty in identifying more sophisticated disinformation campaigns, this could have significant implications for a targeted organisation's reputation.

Looking ahead – cyber threat and risk management in 2021

- The fragmentation of the threat landscape and increasingly blurred boundaries between cyber and other associated risks – including reputational, legal, regulatory and financial – means organisations need to adopt a holistic view of cyber security, involving key stakeholders from across the organisation in the development of cyber risk management and incident response plans.
- The increase in high-impact cyber attacks means that the potential for systemic impacts across an organisation, or even at a national level, is increasing. This places higher demands on organisations to rapidly respond to attacks and increase their level of preparedness and resilience to cyber threats.
- The rapid adoption of digital solutions in response to COVID-19, and the significant connectivity increase resulting from this, has created vulnerabilities across organisations that are difficult to foresee. Organisations need to address these vulnerabilities head on by understanding potential new exposures and gaps across their own systems, assets and people, and by ensuring that safeguards such as cyber due diligence are in place for engagement with third parties.

About us

Control Risks is a specialist risk consultancy that helps create secure, compliant and resilient organisations. We believe that taking risks is essential to success, so we provide the insight and intelligence you need to realise opportunities and grow. And we ensure you are prepared to resolve issues and crises. From the boardroom to the remotest location, we have developed an unparalleled ability to bring order to chaos and reassurance to anxiety.

copenhagen@controlrisks.com controlrisks.com