AI-sammanfattning

När geopolitik blir kod: Cyberangrepp mot Norden i skuggan av ett nytt säkerhetsläge

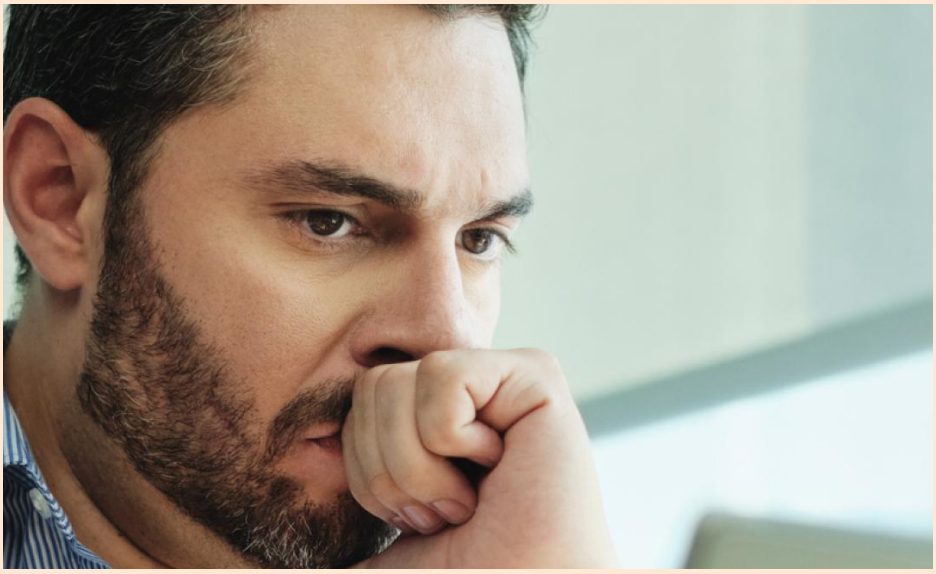
pwc

VOXO

När geopolitik blir kod: Cyberangrepp mot Norden i skuggan av ett nytt säkerhetsläge
Onsdag 24 juni 2026

Sammanfattning

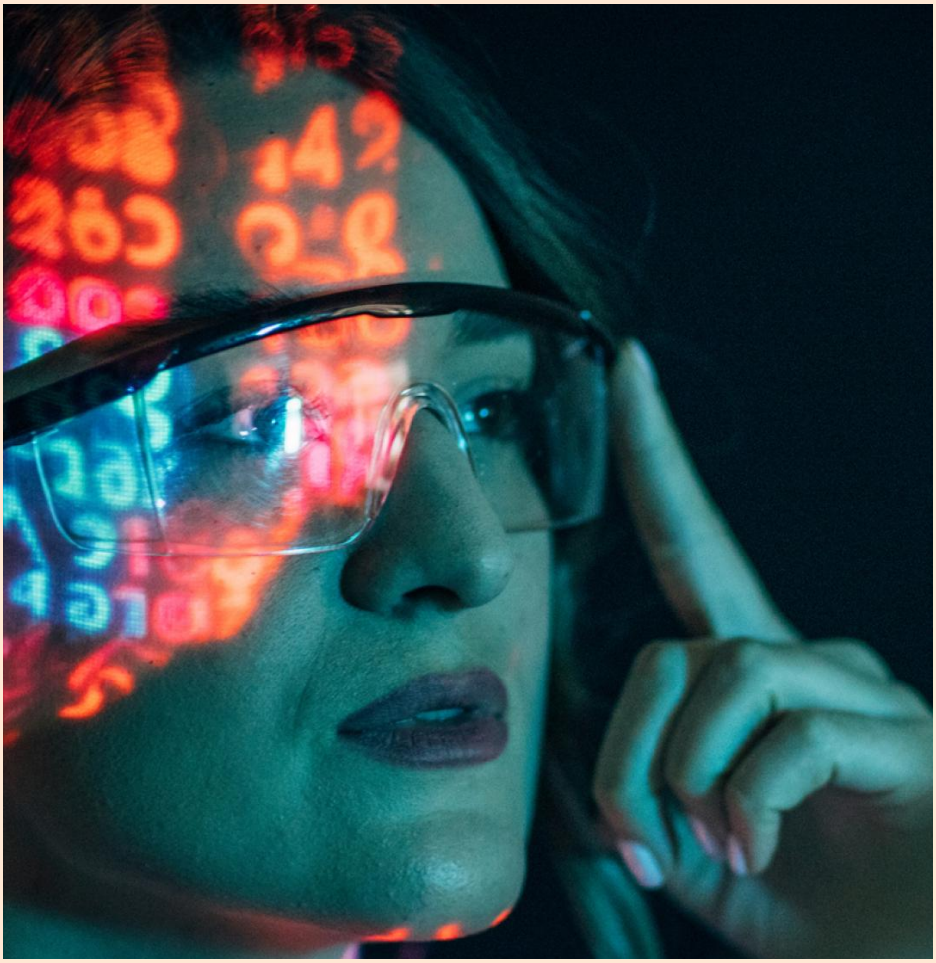
Denna session fokuserade på cyberhot mot Norden i ett skiftande säkerhetspolitiskt landskap och belyste hur dessa hot påverkas av Sveriges Natomedlemskap samt kriget i Ukraina. Sessionen betonade att Norden inte längre fungerar som en neutral buffert mellan Ryssland och Nato, utan har blivit en strategisk måltavla för statssponsrade aktörer. Geografiska områden som Östersjön och Arktis, och sektorer som energi, telekommunikation, och hamninfrastruktur identifierades som särskilt sårbara. Diskussionen berörde också hur AI används av både cyberkriminella och statsstödda aktörer för att utföra sofistikerade och omfattande attacker, där sårbarheter som kablar under vatten och satellitkommunikation ofta är centrala mål. Panelexperterna var eniga om att konsekvenserna av dessa attacker ofta är kaskadeffekter på samhällskritisk infrastruktur, vilket gör robust cybersäkerhet oumbärlig.



Ett stort fokus låg på ledningsorganisationers behov av att anpassa sina incident- och riskhanteringsplaner till de nya hotmodellerna. Petra Klein från Swedbank förklarade hur de skapat en dynamisk säkerhetsstruktur som snabbt kan reagera på nya hot, där prioritering av de mest akuta cyberhoten och översättning av dessa till konkreta åtgärder är centralt. Johan Wiktorin från Intil påpekade samtidigt att många organisationer, särskilt mindre sådana eller de verksamma inom mindre reglerade branscher, saknar tillräckligt skydd mot hot som phishing och ransomware. Några vanliga svagheter inkluderade felkonfigurationer av mejlservrar, okontrollerad informationstillgänglighet och bristande säkerhet kring externa webbsystem. Detta innebär ett ökat utrymme för både innovation och förbättring inom cybersäkerhet.

Geopolitisk påverkan på cyberhot diskuterades också, med betoning på hur statsaktörer som Ryssland, Kina och Iran anpassar sig för att utnyttja nordiska svagheter. Medan Ryssland fokuserar på spionage i energi- och telekomsektorer, söker kinesiska aktörer dominera genom att utnyttja molninfrastruktur och forskningsinnovationer. Samtidigt noterades att iranska aktörer tenderar att utföra reaktiva attacker, ofta kopplade till politiska incidenter som koranbränningar. Nordkoreanska hot fokuserades främst på kryptostölder. Diskussionen visade att dessa aktörers metodik och ihärdighet utmanar både privata och offentliga organisationer att kraftigt förbättra sina försvarsmekanismer och informationsutbyte.

Vad gäller samverkan mellan olika sektorer, betonades vikten av att stärka informationsdelning och koordinering. John Billow från Sveriges Nationella Cybersäkerhetscenter argumenterade för bättre plattformar för att dela tekniska indikatorer och hotinformation, där initiativ på EU-nivå som "cybernav" lyftes fram. Samtidigt pekade Petra Klein på praktiska hinder kring regleringar som begränsar informationsutbyte mellan privata och offentliga aktörer, trots deras samarbete inom forum som NCC:s finansforum. Bättre lagstiftning för att möjliggöra informationsutbyte ansågs avgörande för att skapa en starkare kollektiv försvarskapacitet.



Panelen diskuterade också AI:s inflytande på cybersäkerhet. Medan AI används alltmer av hotaktörer för att skala upp sofistikerade attacker, ansåg panelen att samma verktyg måste utnyttjas av försvarssidan för att hålla jämna steg. Exempelvis kan AI automatisera upptäckt och prevention av hot, men detta kräver bättre governance för att säkerställa ansvarsfull användning. Petra Klein framhöll dock att grundläggande cyberhygien, såsom multifaktor-autentisering och förbättrad identifiering av insiderhot, är kärnan i effektivt skydd. AI-teknologi bör komplettera snarare än ersätta dessa fundamentala processer.

Slutligen diskuterades hur medvetenhet och kommunikation om cybersäkerhet behöver balanseras för att undvika både panik och apati. Initiativ för att höja investeringsnivåer och ledningsengagemang, via cybersäkerhetsregleringar och forum som Finansforum, ansågs lyckade. Men panelen betonade att offentliga och privata aktörer måste agera i symbios för att stärka nationella och sektorsvisa försvar. Det framhölls också att Sverige i framtiden bör satsa på att integrera cybersäkerhet djupt i sin nationella policy och att skapa ett ekosystem som gör svenska organisationer oattraktiva måltavlor för angripare.

När geopolitik blir kod: Cyberangrepp mot Norden i skuggan av ett nytt säkerhetsläge
Onsdag 24 juni 2026

Nyckelinsikter

Nordens ökade geopolitiska exponering kräver stärkt cybersäkerhet

Med Sveriges och Finlands inträde i Nato har Norden gått från att vara en buffertzon till en region med strategisk betydelse, vilket ökar dess sårbarhet för cyberhot. Kritisk infrastruktur såsom energi, telekommunikation och undervattenskablar är särskilt utsatt för hot från statsaktörer och cyberkriminella.

AI förändrar cyberhotens natur och cybersäkerhetsstrategier

Hotaktörer utnyttjar AI för automatiserade attacker, autentiska nätfiskeoperationer och snabbare utnyttjande av systemsvagheter. För att möta dessa hot krävs att AI används även i försvarssyfte, samtidigt som ansvarsroller och incidenthanteringsplaner förbättras.

Samverkan mellan offentlig och privat sektor är essentiell

Panelen betonade vikten av informationsdelning mellan sektorer för att möta cyberhoten effektivt. Samtidigt lyftes hinder till följd av lagstiftningens begränsningar och behovet av bättre samordning mellan myndigheter och företag.

När geopolitik blir kod: Cyberangrepp mot Norden i skuggan av ett nytt säkerhetsläge
Onsdag 24 juni 2026

Deltagare

Charlotte Arnell
PwC

Petra Klein
CISO, Swedbank

Johan Wiktorin
VD, Intil

John Billow
CEO, NCSC Sverige

Matt Carey
Moderator, PwC

Powered by

voxoevent.ai