FoT Strategier i cyberdomänen

Att koka soppa på en cyberspik

Utvecklingar och drivkrafter bakom nordkoreanska operationer i cyber- och informationsdomänen

Frida Edvardsson Lampinen

Nordkorea är ett land förknippat med total informationskontroll, internationell isolering och fattiga levnadsförhållanden. Ändå har den nordkoreanska regimen blivit en framstående hotaktör inom cyber- och informationsdomänen. Nordkoreas cyberoperationer har utvecklats i fyra faser med inledning 2009, följt av 2013, 2016 och 2020. Utvecklingen utmärks av en ökad teknisk mognadsgrad och nyttjande av nya attackvägar, men även av diversifierade målsättningar och en kreativ användning av cybervapen för att bemöta en föränderlig omvärld. Analysen identifierar tre strategiska intressen som ligger till grund för Pyongyangs val av måltavlor och angreppssätt: att säkerställa Kim-familjens politiska makt, att värna statens självbestämmande och att vinna gehör för nationella intressen i internationell politik.

När Nordkorea kommer på tal går tankarna lätt till fattigdom eller politiska utspel. Det är nog få som omedelbart ser framför sig en stat som investerar omfattande resurser i avancerad informationsteknik och datavetenskap. De senaste tio åren har Nordkorea emellertid skapat sig ett rykte som en kompetent, kreativ och framför allt destruktiv cyberhotaktör med förmåga att manipulera, stjäla och förstöra data för att uppnå diverse operativa syften. I en bedömning från 2022 utnämnde forskare på Harvard University Nordkorea till världens 14:e mest framstående cybermakt—med världens bästa förmåga till finansiellt motiverade cyberoperationer.[1]

Inom ramen för FoT-projektet ”Strategier i cyberdomänen” syftar detta FOI Memo att presentera en analys av Nordkoreas cyberverksamhet från ett strategiskt perspektiv. Memot analyserar utvecklingen av Nordkoreas operationer i cyber- och informationsdomänen i förhållande till Nordkoreas strategiska målsättningar och resonerar kring hur Pyongyang använder cybervapen för att komplettera militära, politiska och ekonomiska maktmedel. Analysen i detta FOI Memo demonstrerar hur ett land utan till synes goda ekonomiska och tekniska förutsättningar ändå kan inta en position som betydande hotaktör inom cyberdomänen för att främja sina strategiska mål.

En nordkoreansk elev har lektionstimme i datorkunskap i Pyongyang, 2013.

Källa: Kyodo News via Getty Images.

Ett medfött teknikintresse

Den nordkoreanska ledningen har alltid bevakat ny teknik i syfte att finna nya medel att implementera sin politik. Allt sedan den Demokratiska Folkrepubliken Korea (det formella namnet för Nordkorea) utropades år 1948 har dess styrande ideologi betonat vikten av

1 J. Voo et al. *National Cyber Power Index 2022* (Belfer Center for Science and International Affairs, 2022), ss. 22, 27–30.

FOI Memo 9316
Projektnummer: E12626
Godkänd av: Karolina Gasinska Singh

Juni 2026

politisk självständighet. Syd- och Nordkorea etablerades som konkurrerande politiska alternativ för koreanskt självstyre när den japanska ockupationen avslutades tvärt i och med Japans nederlag i andra världskriget, varför autonomi och rätten till självbestämmande var kärnintressen för båda de nyetablerade staterna. För att undvika att hamna i beroendeställning till sina mecenater Sovjetunionen och Kina institutionaliserade Nordkorea tidigt en strävan efter ekonomisk och teknisk självtillräcklighet, ett koncept som kallas *Juche*.[2] Denna målsättning ska framför allt förstås som ett politiskt ideal, eftersom att Nordkorea i praktiken var beroende av ”vänskaplig handel” (läs: bistånd) med Sovjetunionen fram till sent 1980-tal.[3] Ett centralt budskap i Juche-ideologin är att det nordkoreanska folket kreativt bör utnyttja samhällets samlade resurser för att segra i den revolutionära kampen mot imperialismen.

Viktigt i sammanhanget är att Koreakriget (1950–1953), då Nord- och Syd slogs om ensamrätten för politisk representation av det koreanska folket, avslutades med ett vapenstilleståndsavtal. Därför är både kriget och kampen om självbestämmelse att betrakta som pågående i juridisk mening. Nordkoreansk diskurs tar tillvara på det ständiga hotet om en USA-ledd invasion för att motivera regimens politiska legitimitet. Konflikten beskrivs och upplevs av såväl den politiska eliten som befolkningen som en högst levande, ständigt pågående kamp. Utan Kim-familjens goda ledarskap skulle, enligt detta tänkande, det nordkoreanska folket likt grannarna i syd leva under amerikanskt förtryck och utan rätt till självbestämmande.[4]

I linje med sin strävan efter teknisk självtillräcklighet började Nordkorea tidigt att intressera sig för datorer och informationsteknik (it). Nordkorea tillverkade sin första dator på 1960-talet och under 1970- och 1980-talen etablerades forskningscenter och högskoleutbildningar i datavetenskap.[5] Uppbyggnaden av nationell kompetens genomfördes sannolikt från början med potentiella militärstrategiska tillämpningar i åtanke, men utvecklingen av cybervapen för offensiva syften tycks ha tagit fart ordentligt först under 90-talet. Inspirerad av USA:s informationskrigföring i Kuwaitkriget utfärdade den dåvarande ledaren Kim Jong Il order om att påskynda statens förmågeutveckling inom denna arena.[6] År 1998 etablerade Koreanska folkarmén en cyberenhet inom motsvarande Operationsledningen (*General Staff Department*) i syfte att stärka arméns förmåga att med datorbaserade medel störa, manipulera eller på andra sätt påverka fiendens beslutsprocesser.[7]

Ett land utan internet gör hackerdebut

Samtidigt såg regimen också risker för okontrollerad informationsspridning med den nya tekniken. Nordkorea är en auktoritär stat som utövar strikt informationskontroll. Det finns ingen oberoende press eller media, och straffskalan för införsel eller konsumtion av utländsk media går ända upp till dödsstraff.[8] Under 1990- och 2000-talen betonade statlig medierapportering faror inom it-sfären. Befolkningen uppmanades att iaktta största försiktighet vid användning av datorer och internet framställdes som en laglös plats.[9] Sedan 1996 surfar de allra flesta nordkoreaner uteslutande på det inhemska intranätet som inte är sammankopplat med omvärlden. Nordkorea har visserligen 1 536 IP-adresser[10] med uppkoppling till det globala internet via kinesisk och rysk infrastruktur, men tillgången till dessa är begränsad och reserveras för det politiska toppskiktet.[11] En annan speciell omständighet är att en övervägande

2 National Institute for Unification Education. *Understanding North Korea 2023* (Sydkoreas Återföreningsministerium, 22/8 2024), ss. 31–38.

3 Ibid, ss. 226, 229 och 245.

4 K. Oh & R.C. Hassig. *North Korea: Through the Looking Glass* (Washington D.C.: Brookings Institution Press, 2000).

5 D.A. Pinkston. ‘North Korean Cyber Threats’ i F. Rugge (red.), *Confronting an ‘Axis of Cyber’? China, Iran, North Korea, Russia in Cyberspace* (ISPI, 2018), ss. 94–97.

6 Yoo Pan-deok & Lee Byung-woo. 군사사상 차원의 북한 사이버전 의미와 위협 분석: 북한의‘주체군사사상’과 사이버전을 중심으로 [“Betydelse- och hotanalys av Nordkoreansk cyberkrigföring i ett militärideologiskt sammanhang med utgångspunkt i länken mellan Juche-ideologin och cyberkrigföring”]. 접경지역통일연구 *[Gränsområdes- och återföreningsforskning]* (2023): ss. 269–270.

7 A.H. Cordesman, C. Ayers & A. Lin. *DPRK: Cyber, Electronic Warfare, and SIGINT Capabilities* (CSIS, 2016), s. 25.

8 K.C. Lee. *What is the Reality of Social Control and Punishment in North Korea in the Kim Jong Un Era?* (Korea Institute for National Unification, 2023).

9 An Doo-hwan. 북한의 사이버 안보 담론 연구 [“En studie av Nordkoreansk cybersäkerhetsdiskurs”]. 국방정책연구 *[Försvarspolitisk forskning]*. 39:140 (2023): ss. 90–97.

10 Internet protocol (IP). En IP-adress är knuten till en specifik dator. Som en jämförelse kan nämnas att Sverige har 31,5 miljoner IP-adresser. Siffror hämtade från IP2Location.com (hämtad 13/5 2026).

11 Kong Ji-young, Lim Jong-in & Kim Kyoung-gon. The All-Purpose Sword: North Korea’s Cyber Operations and Strategies. I: *11th International Conference on Cyber Conflict.* (2019), s. 3.

majoritet av nordkoreanska hushåll saknar tillgång till en dator annat än i skolan eller på arbetsplatsen.[12] All datoranvändning sker under partistatens tillsyn och det inhemska operativsystemet *Red Star OS* rapporteras ha inbyggda censur- och övervakningsfunktioner. De få som har en dator måste dessutom registrera den hos de lokala myndigheterna.[13]

Utmärkande för cybervapen är möjligheten att nyttja dem offensivt utan att uppfylla kraven för väpnad konflikt eller en krigshandling. Cybervapen är dessutom svåra att entydigt attribuera, något som angripare kan utnyttja för att förneka sin inblandning och därigenom minska risken för att bli utsatt för motåtgärder.[14] Dessa attribut passar väl in i nordkoreanskt strategiskt tänkande, som är förankrat i en grundläggande preferens för asymmetrisk och irreguljär krigföring: det vill säga användningen av olika kinetiska och icke-kinetiska maktmedel som slår mot fiendens svaga punkter för att framtvinga en önskad politisk utveckling. Nordkorea har sedan 1960-talet utfört diverse sådana operationer för att undergräva stabiliteten i Sydkorea, exempelvis politisk uppvigling och mordförsök på presidenter. År 2009 beslutade Kim Jong Il att samla statliga entiteter som bedrev operationer mot eller i utlandet under ett tak. Sammanslagningen resulterade i bildandet av Generaldirektoratet för underrättelser (*Reconnaissance General Bureau*), en myndighet som saknar direkt motsvarighet i en internationell kontext men har beskrivits som Nordkoreas nav för ”illegal och ljusskygg verksamhet utanför landets gränser”.[15]

Samma år som Generaldirektoratet för underrättelser grundades, 2009, utsattes sydkoreanska och amerikanska myndighets- och företagshemsidor för distribuerade överbelastningsattacker (*distributed denial-of-service* eller *DDoS*) som har attribuerats till nordkoreanska staten.[16] Detta är Nordkoreas första kända externa cyberoperation. Det är inte klarlagt om bildandet av Generaldirektoratet hänger ihop med händelsen. Kärnvapenprogrammet, som utvecklades kraftigt under samma period, stärkte landets förmåga att avskräcka mycket allvarliga militära hot, men är inte lämpligt för avskräckning av icke-existentiella hot. Cybervapen å andra sidan utgör icke-kinetiska attacker som provocerar och stör, men som inte uppnår tröskeln för krig. De fyllde således en lucka i Nordkoreas verktygslåda. Ungefär samtidigt som Generaldirektoratet bildades ska Kim Jong Il ha sagt att kärnvapen och cyberkrigföring tillsammans kan omkullkasta kapitalismen, vilket tyder på att tidpunkten för omorganisationen och DDoS-attacken kan ha ett samband.[17]

En annan tolkning skulle vara att omorganisationen genomdrevs av rent administrativa och styrningsmässiga skäl, men att den samtidigt väckte idéer som ledde till nya samverkansformer och Pyongyangs cyberattacksdebut. I den tidigare organisationen tycks olika verksamhetsområden ha haft begränsad kontakt sinsemellan. Idag förekommer det uppgifter om att olika hotgrupper inom Generaldirektoratet för underrättelser genomför gemensamma operationer där olika grupper ansvarar för olika taktiska moment, snarare än att de ägnar sig åt separata operationer baserat på individuella expertisområden.[18] Oavsett markerar år 2009 startskottet för nordkoreanska operationer i cyberdomänen.

Faser i Nordkoreas cyberverksamhet

Sedan 2009 har nordkoreanska cyberoperationer utvecklats väsentligt avseende modus, medel och ambitionsnivå. Författarens analys visar att utvecklingen kan delas in i fyra faser: experimentell cybervandalism 2009–2012; djärvare exploatering 2013–2015; cyberaktiviteter för ekonomisk vinning 2016–2019; samt professionalisering med operativ bredd sedan 2020 (se tabell 1).[19]

12 Så som är fallet för de flesta fenomen i Nordkorea saknas tillförlitlig statistik. Uppskattningsvis vart femte till vart tredje hushåll äger en dator. Författaren tackar Benjamin Katzeff Silberstein för att ha uppmärksammat mig på detta. Se även S. Moon. North Korea cracks down on unregistered laptops and tablets. *Radio Free Asia* (20/11 2023). *https://www.rfa.org/english/news/korea/laptop-11202023164619.html*

13 3 kap. 26§ och 33§ *Telekommunikationslagen* (2022:1031). Hämtad från *NK Tech Lab, https://www.nktechlab.org/north-korean-law-database/*

14 C. Whyte & B.M. Mazanec. *Understanding Cyber Warfare: Politics, Policy and Strategy* (2:a utgåvan: Routledge, 2023), ss. 85–100. Författaren tackar även FOI-kollegan David Lindahl för att ha påpekat detta.

15 J. Jun, S. LaFoy & E. Sohn. *North Korea's Cyber Operations: Strategy and Responses* (december 2015), ss. 35–45. Citat från s. 35.

16 M. Raska. North Korea's Evolving Cyber Strategies: Continuity and Change. *Sirius*. 4:2 (2020).

17 Yoo Pan-deok & Lee Byung-woo. “Betydelse- och hotanalys av Nordkoreansk cyberkrigföring…”, ss. 269–270.

18 Multilateral Sanctions Monitoring Team [MSMT]. *The DPRK's Violation and Evasion of US Sanctions through Cyber and Information Technology Worker Activities* (22/10 2025).

19 Denna indelning bygger på tidigare forskning som analyserar utvecklingen i tre faser. Den tidigare forskningen är emellertid oense om längden på faserna och berör sällan händelseutvecklingar efter 2022. Se t.ex. Raska. North Korea's Evolving Cyber Strategies; A. Sharma. *North Korea's Cyber Strategy: An Initial Analysis* (ORF, 2024); Kwon Ji-min et al. 북한군사론 *[“Nordkoreansk militärteori”]* (Seoul: Korea Institute for Military Affairs, 2025).

Tabell 1. De fyra faserna i utvecklingen av nordkoreansk cyberverksamhet

Period	Kännetecken	Attackvägar	Huvudsakliga måltavlor
2009–2012	Experimentella attacker, cybervandalism	DDoS	Sydkoreanska och amerikanska myndigheter och försvarssektorer
2013–2015	Djärvare exploatering, utpressning, spionage	Riktat nätfiske, skadlig kod	Sydkoreanska och amerikanska myndigheter; Sony Pictures i USA; sydkoreansk kärnkraft, finanssektor, mediabolag
2016–2019	Cybervapen för ekonomisk vinning och stöld	Hyperanpassat nätfiske, gisslanprogram, vattenhålsattacker, leverantörsattacker	Banker i Sydasien, Latinamerika, decentraliserade finansplattformar (kryptovalutabörser m.fl.)
2020-pågående	Professionalisering, flera parallella kampanjer med olika målsättningar	Förfinande av färdigheter med stöd från generativ AI, dagnollattacker, living-off-the-land	Internationella företag; rysk, kinesisk och sydkoreansk industri; individer med innehav av intressant information oavsett nationalitet

Källa: Tabellen är sammanställd av författaren, se fotnoter i löptexten för källhänvisningar samt förklaring av tekniska begrepp.

Experiment och vandalism, 2009–2012

Den första fasen, cirka 2009–2012, inleddes som nämnts ovan med en överbelastningsattack på sydkoreanska och amerikanska hemsidor. Attacken var inte tekniskt avancerad men genererade likväl uppmärksamhet.[20] Liknande nordkoreanska störningsattacker och även spionage mot sydkoreanska och amerikanska myndigheter fortsatte de följande åren. Kampanjen har fått namnet Operation Troy och beskrivs bäst som cybervandalism.[21] I mars 2011 utsattes sydkoreanska myndighetshemsidor återigen för DDoS-attacker. Operationen var mer tekniskt avancerad än tidigare och kunde ha orsakat större skada än vad som var fallet. Experter menade att attacken kan likställas med att ”ställa upp med en Lamborghini i ett gokart-race”.[22]

De nordkoreanska cyberattackerna fram till 2012 tycks ha genomförts som experiment, dels i form av tekniska metodtester, men framför allt för att undersöka USA:s och Sydkoreas motaktioner och eskaleringsvilja. Nordkorea genomförde dessutom ett antal allvarliga militära provokationer mot Sydkorea under samma period. År 2010 besköt Nordkorea en sydkoreansk ö med artillerield och avfyrade en torped som sänkte en korvett som tillhörde Sydkoreas flotta.[23] Att Pyongyang valde att genomföra cyberattacker när det militära säkerhetsläget var mycket spänt kan ha syftat till att etablera eskalationsdominans och att skaffa sig större förhandlingsutrymme. Cyberattacker tillför en lågintensiv konfliktdimension, vilket sätter ytterligare press på motståndaren men utgör en eskalation som skulle vara relativt smärtfri att avstå i en förhandling för Nordkorea.

Djärvare exploatering, utpressning och spionage, 2013–2015

Den andra fasen, ca 2013–2015, utmärktes av djärvare operationer. Antalet cyberangrepp som attribuerades till Nordkorea ökade samtidigt som operationernas mål och medel diversifierades. Det interna maktskiftet år 2011–2012 då Kim Jong Un tillträdde till makten ger viktig kontext. Kim var ung och i behov av att hävda sin auktoritet gentemot interna kritiker såväl som externa skeptiker. Nytt i verktygslådan var riktat nätfiske (*spear-phishing*), en riktad attack som går ut på att lura individer att släppa in cyberagenter i sitt nätverk genom att öppna bedrägliga hemsidor eller filer. Först identifierar hackarna individer med rätt behörighet, varefter de analyserar vilka typer av kontaktförsök målen är mottagliga för, för att till sist designa och planera en attack anpassad efter målets intressen för att locka dem att ta betet. Angreppssättet användes bland annat 2013 för att infektera sydkoreanska mediabolag med skadlig kod (*malware*). Programmet, som döpts till DarkSeoul, lamslog tiotusentals datorer med stora störningar hos tv-stationer och banker som följd.[24] Riktat nätfiske användes även för att spionera på personer inom de sydkoreanska och amerikanska regeringarna,

20 C.W. Kim & C. Polito. *The Evolution of North Korean Cyber Threats* (The Asan Institute, 2019).

21 R. Sherstobitoff, I. Liba & J. Walter. *Dissecting Operation Troy: Cyberespionage in South Korea* (McAfee, juli 2013). *https://cyber-peace.org/wp-content/uploads/2013/07/wp-operation-troy.pdf*

22 McAfee. *Ten Days of Rain: Expert analysis of distributed denial-of-service attacks targeting South Korea* (juli 2011), s. 12. *https://www.mcafee.com/blogs/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf?msockid=06ac16870241698e3e3d01d403a6682b*

23 K. Korkmaz & J. Rydqvist. *The Republic of Korea: A Defence and Security Primer.* FOI-R--3427--SE (FOI, april 2012), s. 39.

24 D.M. Martin. *Tracing the Lineage of DarkSeoul* (SANS Institute, 4/3 2015). https://www.sans.org/white-papers/36787

militären, försvarsföretag, universitet och tankesmedjor, och kärnkraftssektorn med flera.[25]

Den enskilt mest uppmärksammade incidenten inträffade i november 2014 i samband med biopremiären av den amerikanska satirfilmen *The Interview*. Filmen handlar om två amerikanska journalister som reser till Nordkorea för att lönnmörda landets ledare. Filmen väckte stor anstöt i Pyongyang som i protest attackerades bolaget bakom filmen, Sony Pictures, med ett program som satte företagets interna datasystem ur funktion. Utöver de tekniska och ekonomiska skador som detta orsakade kom hackarna åt en mängd känsliga dokument som sedan i omgångar läcktes till media i utpressningssyfte. I slutändan misslyckades operationen med att förhindra filmens utgivning. Några dagar innan den planerade premiären hotade hackergruppen med fysiska terrordåd på biografer i USA, vilket visserligen fick Sony Pictures att stoppa filmen, men eskaleringen innebar också att hotet utvecklades till en nationell angelägenhet. President Barack Obama fördömde incidenten som ett hot mot yttrandefriheten och utlovade amerikansk vedergällning om hotet realiserades. Politiseringen av händelsen ledde till att USA etablerade eskalationsdominans och Pyongyang tvingades att backa från sina krav. Filmen hade premiär och den stora uppmärksamheten bidrog till att den därtill blev en publiksuccé.[26]

Cyberstöld och vinstdrivande verksamhet, 2016–2019

Genom Sony-incidenten tycks Nordkorea ha insett begränsningarna med att använda cyberangrepp i politiska syften. Den tredje fasen, ca 2016–2019, medförde en fortsatt hög aktivitetsnivå, om än med lägre politisk profil. Påverkanskampanjer med syftet att sprida Nordkorea-vänliga budskap å ena sidan och förstärka motsättningar inom alliansen mellan Sydkorea och USA å andra sidan bedrevs intensivt på alla stora sociala medieplattformar.[27] Inom cyberspionagespåret prioriterades stöld av militära och vapentekniska dokument, medan spridningen av gisslanprogrammet (*ransomware*) WannaCry, som 2017 paralyserade tiotusentals datorer i 150 länder, sådde oro och undergrävde tilliten till samhällelig digitalisering.[28]

Den ledande målsättningen för cyberverksamheten vid den här tiden tycks dock ha varit att tjäna pengar. År 2016 genomförde Nordkorea sitt första storskaliga digitala rån. Genom att manipulera banköverföringssystemet SWIFT kom nordkoreanska hackare åt 81 miljoner US-dollar från Bangladesh riksbank. Fram till 2019 försnillade Nordkorea åtminstone en halv miljon US-dollar från en bank i Taiwan, 15 miljoner dollar från latinamerikanska banker, och 13 miljoner euro från Bank of Valletta.[29] Flera av dessa rån genomfördes genom riktat nätfiske med en högre grad av individanpassning än tidigare. Exempelvis kontaktade hackarna en anställd på en chilensk bank på LinkedIn, bjöd in denne till en falsk online anställningsintervju, och lurade därigenom den anställde att ladda ner filer med skadlig kod som gav tillgång till bankens nätverk. Även så kallade vattenhålsattacker användes för att infiltrera banknätverk. Denna metod går ut på att skadlig kod placeras på webbsidor som den tilltänkta målgruppen ofta besöker i förhoppning om att infektera ”rätt” persons dator.[30]

Den nya inriktningen sammanföll med en kraftig nedgång i nordkoreansk ekonomi. Statsfinanserna har alltid varit magra men situationen förvärrades när FN:s säkerhetsråd åren 2016–2017 införde stränga sanktioner på handel med Nordkorea för att markera mot regimens kärnvapentester. Exportvolymen störtdök från 2,83 miljarder US-dollar 2016 till knappt 243 miljoner dollar år 2018, en minskning med 91,5 procent.[31] Det är inte första gången som regimen använder sig av brottslighet för att dryga ut statskassan. Nordkoreanska tjänstemän har i flera årtionden sysslat med bland annat drogtillverkning, tobaks- och vapensmuggling, samt valutaförfalskning

25 S.H. Lee. Revisiting the 2014 Korea Hydro and Nuclear Power Hack: Lessons Learned for South Korean Cybersecurity. *38 North* (22/3 2024). *https://www.38north.org/2024/03/revisiting-the-2014-korea-hydro-and-nuclear-power-hack-lessons-learned-for-south-korean-cybersecurity/*

26 G. White. *The Lazarus Heist* (Penguin Books, 2022), ss. 75–100; B. Buchanan. *The Hacker and the State* (Harvard University Press, 2020), s. 184.

27 D.A. Pinkston. Inter-Korean Rivalry in the Cyber Domain: The North Korean Cyber Threat in the ‘Sŏn’gun’ Era. *Georgetown Journal of International Affairs*. 17:3 (2016); S. Bradshaw, H. Bailey & P.N. Howard. *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation* (Project on Computational Propaganda, 2021).

28 Z. Cohen. North Korean hackers stole US-South Korea war plans, official says. *CNN* (11/11 2017). *https://edition.cnn.com/2017/10/10/politics/north-korea-hackers-us-south-korea-war-plan/index.html*

29 UNSC. *Report of the Panel of Experts established pursuant to resolution 1874 (2009)*. 2019:691 (2019), ss. 109–110. *https://docs.un.org/en/S/2019/691*; B. Borg, V. MacDonald & C. Caruana. BOV goes dark after hackers go after €13m. *Times of Malta* (13/2 2019). *https://timesofmalta.com/article/bank-of-valletta-goes-dark-after-detecting-cyber-attack.701896*

30 UNSC. *Report of the Panel of Experts established pursuant to resolution 1874 (2009)*, ss. 27, 113.

31 Sydkoreanska statistikministeriet. 북한의 품목별 수출입액 *[“Nordkoreanska handelsvolymer per produktkategori”]* (13/8 2025); FN:s säkerhetsrådsresolutioner nr. 2321 (30/11 2016) och 2397 (22/12 2017).

i syfte att tjäna pengar.[32] Cyberbrottslighet tillåter gärningspersoner att dölja sin identitet och att slå till mot geografiskt avlägsna platser, vilket fördröjer och försvårar utredning och lagföring av brotten.

Digital stöld av reella finansiella tillgångar är dock fortfarande krävande. Pengarna måste tvättas och i detta syfte använder sig Nordkorea av mellanhänder i länder som Kina, Ryssland, Argentina, Kambodja, Förenade Arabemiraten och Myanmar. Mutor och avgifter ska betalas i varje steg av processen vilket gör att det slutliga stöldbytet krymper avsevärt. Detta är en förklaring till varför operationerna har expanderat till den decentraliserade finanssektorn. Sedan 2017 har Nordkorea genomfört uppskattningsvis ett femtiotal kupper mot företag som hanterar kryptovalutor med en samlad vinst på uppemot 6,6 miljarder US-dollar.[33] Summan av stulen kryptovaluta år 2024 motsvarade ca 15 procent av Nordkoreas uppskattade militära utgifter. Värdet av landets totala export samma år motsvarade bara ca 3,5 procent av de militära utgifterna.[34] Stulen kryptovaluta förs sannolikt aldrig in i Nordkorea, utan används för att i utlandet inhandla, och därefter smuggla in, varor som landet inte får direktimportera.

Professionalisering och parallella kampanjer, 2020-pågående

År 2020 drabbades världen av coronapandemin. Nordkorea var inget undantag. Landets huvudsakliga smittskyddsåtgärd var att stänga gränserna helt och varken handelsvaror eller personer kom in eller ut under åren 2020–2023.[35] Pandemihanteringens höga politiska prioritet speglades även i cyberverksamheten. Den fjärde fasen av nordkoreanska cyberoperationer, från 2020 tills idag, präglas av kreativ problemlösning varigenom dataintrång, sabotage och stöld genomförs på nyskapande sätt för att uppnå politiska mål. Ett första problem som Nordkorea ställdes inför under pandemin var behandling av coronaviruset. Nordkoreas sjukvårdssystem är resurssvagt och det råder brist på läkemedel även under normala omständigheter. Enligt uppgift beordrades statsförvaltningen under senhösten 2020 att fokusera på införskaffningen av vaccin och under samma period började nordkoreanska hackare att utsätta internationella företag och hälsomyndigheter med kunskap om vaccintillverkning för dataintrång.[36] När det värsta hotet väl hade passerat omdirigerades cyberspionageverksamheten till att stödja regimens ekonomiska politik. Dataintrång hos sydkoreansk tillverkningsindustri har ökat markant sedan Kim Jong Un 2024 lanserade en policy med målsättningen att blåsa liv i landsbygden genom att bygga ett stort antal nya fabriker.[37]

En annan effekt av gränsstängningen var att nordkoreaner som arbetade i utlandet inte kunde resa hem, samtidigt som utlandsposteringar fick minskad finansiering från Pyongyang. Analytiker har tolkat den ökning som har skett av småskalig cyberstöld sedan 2020 som en direkt effekt av att statlig verksamhet utanför centralregeringen i högre grad än tidigare har behövt vara självfinansierad.[38] Omfattningen av Nordkoreas kryptovalutastölder har också ökat sedan 2020. Kryptovalutor har blivit mer populära och växelkurserna har stigit, vilket innebär att kryptostölder lönar sig bättre, men tillgängliga data antyder även att Nordkorea även använder sig av mer innovativa metoder. Kommersiella AI-tjänster används för att vässa trovärdigheten av riktade nätfiskeförsök och räckvidden av en lyckad infiltration kan omfatta fler offer genom leverantörsattacker.

Nordkoreanska cyberagenter tycks också oftare än tidigare framgångsrikt utnyttja dagnoll-sårbarheter (så kallade *zero-days*) i målets programvara för att installera skadlig kod eller manipulera befintlig kod att utföra skadliga funktioner utan installation av extern kod (*living-off-the-land*). Det tyder på en ökad teknisk kompetens.[39] Hackarnas tekniska framsteg kan kopplas

32 J. Park. *Cyber-hacking as a Means of "Self-reliance": North Korea's Ransomware-based Cyber-hacking for Economic Gains in the Absence of Regulations on Cryptocurrencies in Global Finance* (National Committee on North Korea & Wilson Center, 2022).

33 MSMT. *The DPRK's Violation and Evasion of US Sanctions...* ss. 24–26, 42–49.

34 Beräkning av författaren baserat på uppgifter från Sydkoreanska statistikministeriet om nordkoreanskt BNP och exportvärden samt uppgifter från MSMT om summan av kryptostöld.

35 V. Cha, K. Katz & S. Ji. *Behind Shuttered Borders: A view into North Korea's COVID-19 experiences* (CSIS, juni 2025). *https://www.csis.org/analysis/behind-shuttered-borders*

36 S. Jang. North Korean leadership orders public health officials to focus all efforts on vaccine acquisition. *Daily NK* (21/12 2020). *https://www.dailynk.com/english/north-korean-leadership-orders-public-health-officials-focus-all-efforts-vaccine-acquisition/*

37 Hong Jun-ki & Park Sang-jung. 북한의 사이버전 역량변화와 위협 전망: 군사적 관점을 중심으로 ["Utvecklingsriktning för Nordkoreas cyberkrigsförmåga och hot från ett militärt perspektiv"]. *The Journal of Social Convergence Studies*. 8:6 (2024): s. 97.

38 M. Barnhart. *Exposing DPRK's Cyber Syndicate and Hidden IT Workforce* (DTEX, 2025), s. 28.

39 S. Reddy. Google says North Korean cybercriminals have stepped up 'misuse' of its AI tools. *NK News* (7/11 2025). *https://www.nknews.org/2025/11/google-says-north-korean-cybercriminals-have-stepped-up-misuse-of-its-ai-tools/*; M. Faou. Supply-chain attack on cryptocurrency exchange gate.io. *Welivesecurity* (6/11 2018). *https://www.welivesecurity.com/2018/11/06/supply-chain-attack-cryptocurrency-exchange-gate-io/*

till Kim Jong Uns stora satsningar på att öka landets kompetens inom vetenskap och teknik. Kim har drivit linjen att göra Nordkorea till en vetenskapsnation sedan makttillträdet 2012, men forskning och teknikutveckling har fått en ännu mer framträdande roll i politiken om ekonomisk självtillräcklighet sedan 2021.[40]

Bedrägligt förvärvsarbete inom it-sektorn ökade kraftigt vid den här tiden, och är ett tydligt exempel på Nordkoreas förmåga att anpassa sina metoder efter rådande omständigheter. Uppskattningsvis 2 000 nordkoreaner huvudsakligen bosatta i Kina och Ryssland arbetar under falska identiteter åt internationella företag som bland annat mjukvaruutvecklare. Arbetet de utför är genuint och lönen de mottar i utbyte likaså. Detta arbetssätt tycks ha förekommit sedan ca 2018, men har ökat i och med att distansarbete blev vanligare. Under 2024 tjänade nordkoreanska staten 350–800 miljoner US-dollar genom löneutbetalningar för distansarbete.[41]

Nordkoreanskt nätfiske och distansarbete uppvisar en över förväntan god förståelse för omvärlden, landets isolering till trots. Cybersoldaterna tycks ha god kännedom om olika sociala medieplattformar och hur de används, till synes utan att deras politiska övertygelse eller arbetsvilja påverkas av tillgången till ocensurerad information. Förståelsen är emellertid långt ifrån perfekt och nordkoreanska agenters bristande språk- och kulturella kompetens har i flera fall lett till att deras identiteter uppdagats.[42] I och med att nordkoreanskt distansarbete uppmärksammas allt mer kommer arbetssökande att ställas inför striktare kontroller, vilket betyder att nordkoreanska ansökande behöver kunna uppträda friare och mer naturligt. Samtidigt har Kim Jong Un infört hårade straff för konsumtion av icke-statlig information. I värsta fall kan nyfikenhet på omvärlden och utländsk media leda till dödsstraff.[43] Således framstår det som osannolikt att cybersoldater kommer att tillåtas (eller våga!) leva sig in i sina antagna identiteter till en trovärdig grad, en balansgång som kan bli en utmaning framöver.

Strategisk nytta och utvecklingsriktning

Nordkoreanska cyberoperationer bedrivs inom olika spår parallellt. Uppskattningsvis 25 procent av verksamheten går ut på informationspåverkan, 20 procent på digitala stölder, 20 procent på teknisk underrättelseinhämtning och industrispionage och resterande 15 procent på politisk- och militär underrättelseinhämtning.[44] Fördelningen mellan dessa olika spår säger dock inte så mycket om de långsiktiga, strategiska målsättningarna. I diskussioner om nordkoreanska hot är det lätt att avfärda landet som en irrationell eller oseriös internationell aktör som stör andra utan särskild målsättning, förmåga eller intresse att orsaka större skada. Denna uppfattning är långt ifrån verkligheten. Trots att Pyongyangs uppträdande kan vara svårt att begripa sig på så är landets agerande tydligt förankrat i nationella strategiska intressen. Författaren bedömer att nordkoreanska cyberoperationer uppfyller tre strategiska mål som speglar olika aspekter av att säkerställa statens överlevnad i en osäker omvärld.

Det första målet är att säkra familjen Kims maktställning. Regimens överlevnad handlar inte bara om att det nordkoreanska politiska systemet måste motstå demokratisering, utan om att Kim-familjen specifikt ska behålla sin absoluta makt. Cyberverktyg bidrar till att forma inrikes- och utrikes informationsmiljöer utefter regimens intressen. Genom censur och övervakning bibehåller staten inrikes informationskontroll och undanröjer narrativ som utmanar regimens legitimitet. Nordkoreanska påverkansoperationer utomlands avser bland annat att försvaga Sydkoreas försvars- och utrikespolitiska relationer och därigenom i förlängningen Seouls politiska vilja att angripa Nordkorea. Även cyberspionage mot sydkoreanska och amerikanska militära och politiska mål hjälper Nordkorea att förbereda sig på att hantera en potentiell kris- eller krigssituation.

Det andra målet är att upprätthålla statens politiska autonomi och garantera Nordkoreas rätt till självbestämmande. Juche-ideologin är mycket tydlig i sitt budskap: Nordkorea måste eftersträva ekonomisk, politisk och teknisk självtillräcklighet för att inte hamna i beroendeställning till främmande makt. Det anses bättre att

40 Nordkoreas Utrikesministerium. Great Programme for Struggle Leading Korean-style Socialist Construction to Fresh Victory: On Report Made by Supreme Leader Kim Jong Un at Eighth Congress of WPK. *KCNA Watch* (9/1 2021). *https://kcnawatch.org/newstream/1610272851-580631610/great-programme-for-struggle-leading-korean-style-socialist-construction-to-fresh-victoryon-report-made-by-supreme-leader-kim-jong-un-at-eighth-congress-of-wpk/*

41 MSMT. *The DPRK's Violation and Evasion of US Sanctions...* ss. 7–8.

42 T. Rebane et al. Inside North Korea's Efforts to Infiltrate US Companies. *CNN* (5/8 2025). *https://edition.cnn.com/interactive/2025/08/05/world/north-korea-it-worker-scheme-vis-intl-hnk/index.html*

43 Lee. *What is the Reality of Social Control and Punishment in North Korea in the Kim Jong Un Era?*

44 S.Y. Lee & H.U. Hwang. Digital warfare: N. Korea's evolving cyber arsenal and global threats. *Daily NK* (28/3 2025). *https://www.dailynk.com/english/digital-warfare-north-korea-evolving-cyber-arsenal-global-threats/?tztc=1*

ägna sig åt stöld än att vara biståndsmottagare—i den nordkoreanska socialistiska revolutionens namn är alla medel tillåtna. Cyberdomänen är en lukrativ miljö för digital stöld- och bedrägeribrottslighet som inte kräver någon fysisk närvaro på plats och därmed innebär en låg risk för att åka fast. Teknisk information som inhämtas genom cyberspionage driver den inhemska industriutvecklingen framåt och ger regimen något att visa upp för befolkningen som bevis på sin påstådda oumbärlighet för nationens relativa välstånd.

Det tredje målet är att vinna gehör för nationella intressen i internationell politik. Nordkoreas internationella utanförskap och låga status gör att Pyongyang kämpar i uppförsbacke för att få det globala samfundet att ta dess intressen på allvar, speciellt i frågor som berör relationen med Sydkorea. Seoul åtnjuter ett internationellt legitimitetsövertag. Nordkoreas långsiktiga mål tycks vara att förankra regimens politiska legitimitet internationellt—framför allt med USA— som ett slags försäkring mot militära angrepp för att skapa sig politiskt andrum att fundera på andra frågor än överlevnad.

Nordkorea har länge sökt status och förhandlingsstyrka genom utvecklingen av kärnvapen, men erkännande som legitim kärnvapenmakt har uteblivit. Under tiden har landet försatt sig själv i allt djupare diplomatisk och ekonomisk isolering. Det kan tyckas paradoxalt att en stat som söker legitimitet till synes inte bryr sig om normer kring hur stater normalt bör uppträda. Denna motsättning kan förstås som en självbevarelsemekanism inom vilken Nordkorea drar nytta av sitt rykte som oberäknelig för att avskräcka andra länder från aggressiva handlingar, något som regimen ser som ett reellt hot tills den dagen då landet kärnvapenstatus erkänns internationellt. Samtidigt vill inte regimen vänta med att påverka internationell politik tills att denna målbild går i uppfyllelse. Det är inte trovärdigt att hota med kärnvapen i varje konflikt- eller förhandlingssituation, medan Nordkoreas normalt hårda retorik gör att diplomatiska utspel har svag effekt. Pyongyang har därmed ett behov av avskräcknings- och tvångsmedel som kan göra viss skada och som regimen trovärdigt kan hota med att använda i fredstid, ett snäpp upp från hotfulla uttalanden och robottester. I detta sammanhang är cybervapen användbara för att störa infrastruktur och samhällstjänster eller stjäla känsliga data i utpressningssyfte.

Kompetensförsörjning för cyberverksamheten tycks vara högt prioriterad, vilket talar för en fortsatt utveckling av Nordkoreas förmåga att genomföra offensiva cyberoperationer. Det nordkoreanska samhället erbjuder inte fria karriärval, utan medborgare utbildas och tilldelas anställning utifrån noggranna beräkningar av hur mycket arbetskraft som staten behöver inom olika verksamhetsområden.[45] Tillgängliga uppgifter tyder på att rekryteringskvoten för cybersoldater har höjts. Elever på låg- och mellanstadiet som uppvisar talang för matematik och datorkunskap placeras i spetsprogram och de bästa utbildas sedan vidare på något av landets tre toppuniversitet. Nordkorea tillämpar ett klassystem som delar in befolkningen i tre lojalitetsgrupper och ger individer olika rättigheter utifrån bedömd politisk lojalitetsgrad. Tidigare var enbart barn i den finaste politiska klassen berättigade för cyberutbildning. Sedan 2023 ska emellertid även barn från de lägre politiska klasserna kunna bli utvalda.[46] Detta kan tolkas som att talangförsörjningen för cyberverksamheten är så pass prioriterad att Kim Jong Un är villig att rucka på den grundläggande samhälleliga ordningen.

Sammanfattningsvis skiljer sig nordkoreanska operationer i cyber- och informationsdomänen från andra staters på två huvudsakliga punkter. För det första är Nordkoreas cyberverksamhet bred och bedrivs mot flera parallella mål samtidigt men med ovanligt stor framgång inom finansiellt motiverad cyberbrottslighet. Valet av måltavlor tycks vara opportunistiskt och pragmatiskt, det vill säga att man angriper aktörer som besitter information av värde eller finansiella resurser oavsett nationalitet med fokus på måltavlor med sämre cybersäkerhetsrutiner. För det andra har nordkoreansk cyberkapacitet utvecklats mycket snabbt avseende teknisk kompetens trots landets dåliga ekonomi och isolering. Nordkorea har förstått att den svagaste länken i cybersäkerhet är användaren och de cyberoperationer som röner störst framgångar använder riktat nätfiske hyperanpassat efter individen.

Slutligen tycks förklaringen till Nordkoreas utveckling som cyberhotaktör ligga i en strategisk kultur som värdesätter kreativt resursutnyttjande för att lösa politiska problem, drivet till sin spets i en mycket resurssvag stat med många utmaningar. En bred tillämpning av cyberverktyg för att lösa diverse politiska problem tillåter Nordkorea att koka soppa på en spik och överleva i en osäker omvärld. ■

45 M. Yoon. How do you get a job in North Korea? *NK News* (29/11 2013). *https://www.nknews.org/2013/11/how-do-you-get-a-job-in-north-korea/*

46 Hong Jun-ki & Park Sang-jung. "Utvecklingsriktning för Nordkoreas cyberkrigsförmåga…", ss. 99, 103.