# Förutsättningarna för digitalt samarbete inom Brics

Per-Erik Nilsson och Carolina Vendil Pallin (red), David Lindahl, Olivier Milland, Samuel Neuman Bergenwall, Anna Ida Rock

FOI-R--5776--SE

Juni 2026

# Förutsättningarna för digitalt samarbete inom Brics

Per-Erik Nilsson och Carolina Vendil Pallin (red),
David Lindahl, Olivier Milland, Samuel Neuman
Bergenwall, Anna Ida Rock

| | |
|---|---|
| Titel | Förutsättningarna för digitalt samarbete inom Brics |
| Title | Cooperation on digital affairs the inside BRICS |
| Rapportnummer | FOI-R--5776--SE |
| Månad | Juni |
| År | 2026 |
| Antal sidor | 122 |
| ISSN | 1650-1942 |
| Kund | Försvarsdepartementet |
| Forskningsområde | 8. Säkerhetspolitik |
| Projektnummer | E12626 |
| Godkänd av | Måns Nilsson |
| Ansvarig avdelning | Försvarsanalys |

Omslagsbild: President Vladimir Putin deltar i Bricstoppmötet i Rio de Janeiro den 8 september 2025 från sitt residens i Sotji. Putin är förhindrad att resa eftersom han är internationellt efterlyst för krigsbrott. Kinas president, Xi Jinping, ses på skärmen. Vyacheslav Prokofyev, Sputnik, Kremlin Pool Photo via AP.

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk, vilket bl.a. innebär att citering är tillåten i enlighet med vad som anges i 22 § i nämnd lag. För att använda verket på ett annt sätt som inte medges direkt av svensk lag krävs särskild överenskommelse.

# Sammanfattning

Den tekniska utvecklingen har gjort cyberfrågor centrala i många länders säkerhetspolitik, inte minst Ryssland som vill fördjupa det digitala samarbetet inom Brics (innan 2024 bestående av Brasilien, Ryssland, Indien, Kina och Sydafrika). Rapporten undersöker (1) Bricsländernas val av cyberinfrastruktur; (2) hur dessa val motiveras säkerhetspolitiskt; (3) hur länderna ställer sig till ett fördjupat digitalt samarbete inom Brics; samt (4) vilka åtgärder länderna har vidtagit och förespråkat för att reglera internet.

Kinas ekonomiska styrka och teknologiska utveckling gör landet till en dominant aktör inom Brics och Peking vill, liksom Ryssland, försvaga västs inflytande och öka statlig kontroll över internet. Även Brasilien, Indien och Sydafrika vill minska västlig dominans i globala institutioner, men inte helt fjärma sig. Istället kommer de sannolikt fortsätta balansera utrikespolitiskt för att säkerställa tillgång till teknik från å ena sidan väst, å andra sidan Kina.

Framöver kommer USA:s politiska agerande och Bricsländernas inrikespolitiska vägval att påverka benägenheten att fördjupa det digitala samarbetet. Utvidgningen av Brics påverkar dynamiken inom organisationen och de infrastrukturval medlemsländerna gör framöver kommer bli avgörande. Än så länge är det digitala samarbetet begränsat, men faktorerna ovan får konsekvenser för huruvida internet kommer att utvecklas mot ökad fragmentering i säkerhetspolitiska block.

# Summary

Cyber issues are a core national security policy concern in many countries, not least Russia which is seeking deeper digital cooperation within BRICS (prior to 2024 consisting of Brazil, Russia, India, China and South Africa). This report examines (1) the cyber infrastructure choices made by BRICS members; (2) their justifications for these choices; (3) these countries' inclination to deepen digital cooperation; and (4) their proposed or implemented measures to regulate the Internet.

China's economic power and advanced technological development make it a dominant actor within BRICS, and Beijing, like Moscow, aims to weaken Western influence and increase state control over the Internet. While Brazil, India and South Africa also want diminish Western dominance, they stop short of distancing themselves completely from the West. Instead, their foreign policy hedging allows them to secure access to both Western and Chinese technology.

Future U.S. policies, along with the BRICS countries' domestic policy choices, will influence the likelihood of deepening digital cooperation. Furthermore, the inclusion of new members will impact the internal BRICS dynamics, and the infrastructure choices made by its members will be key. So far, digital cooperation remains limited, but the factors abovementioned will affect whether the Internet will fragment along geopolitical fault lines.

# Förord

Denna studie är skriven för Försvarsmakten inom projektet Strategier i cyberrymden och syftar till att undersöka förutsättningarna för ett fördjupat samarbete digitalt samarbete inom ramen för Brics. Den är ett resultat av samarbete mellan teknisk kompetens på it-området och säkerhetspolitisk kompetens för länderna som ingår i Brics: Brasilien, Ryssland, Indien, Kina och Sydafrika. Som redaktörer kan vi inte nog tacka alla som bidrog med sin expertis och kunnande och då inte minst författarna trots pressat tidsschema: David Lindahl (it-säkerhet och internets struktur); Olivier Milland (Brasilien); Samuel Neuman Bergenwall (Indien) och Anna Ida Rock (Sydafrika).

Rapporten ska förhoppningsvis kunna bidra till att lägga en grund för framtida jämförelser och analyser av Bricsländerna på det digitala området och för studier om huruvida vi går mot en mer uppdelad teknikutveckling och ett splittrat internet som ett resultat av dagens säkerhetspolitiska utveckling.

Författarna vill särskilt tacka professor Bo Petersson vid RUCARR på Malmö universitet, Henrik Karlzén på Cyberförsvar och ledningsteknik och Mattias Svahn på Försvarsanalys som granskade rapporten vid ett seminarium den 2 juni 2025. Som redaktörer hade vi enorm hjälp också av David Lindahls slutläsning av samtliga kapitel med ”teknikglasögonen” på. Samtligas kloka synpunkter och noggranna genomgång ledde till att rapporten förbättrades avsevärt. Ett stort tack går också till Mattias Burell (Försvarsanalys) som gjorde en första granskning av Kinakapitlet under våren 2025. Ett varmt tack går till Karin Blext som bidrog med proffsigt layoutstöd.

Vi har valt att använda ett förenklat fotnotssystem (där vi inte inkluderar URL-er eller översättningar titlar på verk eller datum då vi hämtat något på internet), men inkluderar fulla referenser i referenslistor sist i varje kapitel. Vi har även en förkortningslista (se s. x) och en lista över storlek och mått (se s. x) som används i rapporten för att underlätta läsningen.

Per-Erik Nilsson och Carolina Vendil Pallin, juni 2026

# Sammanfattning

Organisationen Brics, sedan 2010 bestående av länderna Brasilien, Ryssland, Indien, Kina och Sydafrika, avfärdades länge av västliga analytiker som oväsentlig. Med alltmer motsättningar och konfrontation internationellt finns dock anledning att ägna Brics-ländernas samarbete mer uppmärksamhet. Framför allt Ryssland och viss mån även andra Brics-länder har fört fram olika initiativ för att nå ett närmare samarbete på det digitala området. I takt med att cyberdomänen får allt större betydelse skulle ett Brics som samarbetar närmare på det digitala området innebära att en stor andel av världens befolkning använder annan teknisk infrastruktur och andra digitala lösningar jämfört med i väst. Det skulle innebära att säkerhetspolitiska överväganden leder till en cyberdomän som är mer uppdelad politiskt och geografiskt. En sådan utveckling skulle i sin tur på sikt kunna bidra till att cementera splittringen mellan världens ekonomiska och militära stormakter i säkerhetspolitiska block.

I vilken utsträckning driver de ursprungliga Brics-länderna en gemensam agenda för att skapa ett framtida och separat Brics-internet? För att svara på den frågan finns anledning att undersöka: (1) Vilka infrastrukturella val varje ursprungligt Brics-land har gjort; (2) Hur det enskilda landet motiverar dessa val säkerhetspolitiskt; (3) Vilken position landet intar i relation till en gemensam internetpolitisk hållning i inom Brics; samt (4) Vilka enskilda initiativ (om några) som landet har tagit vad gäller i relation till styrning och reglering av internet drivs?

Brics startade som ett mötesformat i marginalen, men har med tiden fått en mer etablerad form. Brics har inget geografiskt högkvarter eller permanent kansli, utan bygger på ett roterande ordförandeskap och ett dynamiskt samarbete format utifrån aktörernas individuella intressen inom ett område. Ett sådant område är cybersäkerhet och digital utveckling. Den 1 januari 2024 upptog Brics dessutom ett antal nya medlemmar, Egypten, Etiopien, Förenade Arabemiraten, Indonesien och Iran, och blev därmed vad som kommit att kallas Brics+. Totalt omfattar Brics-länderna därmed nästan hälften av världens befolkning och en allt större andel av dess bruttonationalprodukt (BNP). Framför allt Kina, men i allt högre grad även Indien, svarar för en stark BNP-utveckling inom Brics.

## Brics-länderna och digitalt samarbete

För Brasilien är Brics ett sätt att stärka landets status internationellt och i sitt närområde. Liksom Kina och Ryssland vill Brasilien utmana rådande globala maktstrukturer, dock utan att kapa banden till väst. Brasilien vårdar sin strategiska autonomi och utrikespolitiska tradition av alliansfrihet. Till skillnad från Kina och Ryssland är Brasilien dessutom fortfarande en demokrati, om än med vissa inskränkningar av internetfriheten. Kuppförsöket den 8 januari 2023 innebar att Brasilien kom att fokusera ännu mer på interna hot. På cyberområdet innebär det att regleringar och begränsningar i de logiska och cyberpersona-lagren i cyberdomänen.

Handeln med Kina har bidragit väsentligt till Brasiliens tillväxt, men den har också medfört en ökad sårbarhet för internationella konjunktursvängningar inte minst när dessa involverar Kina. Brasilien försöker därmed diversifiera sina samarbeten, t.ex. på försvarsområdet med västliga länder. Målet är att bygga en mer tekniskt avancerad industri, genom teknik- och teknologiöverföring. När Brasilien nu bygger ut femte och sjätte generationens mobiltelefoni så fortsätter landet att balansera mellan risker och fördelar med att förlita sig på kinesiska företag. Å ena sidan har USA utövat påtryckning för att begränsa Kinas roll i den pågående infrastrukturutbyggnaden, å den sidan andra erbjuder Kina teknisk utveckling till lägre kostnader.

Ryssland drev tidigt på för att Brics skulle gå från att vara ett prefix för länder med stark tillväxt till att bli ett organiserat mötesformat. På cyberområdet ligger Ryssland dessutom bakom en rad initiativ, bland annat för att mobilisera stöd för internationellt bindande avtal om informationssäkerhet inom FN. Liksom Kina vill Ryssland etablera kontroll över det man definierar som en rysk informationssfär. Det har skett genom en rad åtgärder, bland annat genom lagstiftning för att etablera ett ”suveränt internet”.

Trots ryska förslag om en rad samarbetsformat på det digitala området inom Brics så är det svårt att peka på praktiska resultat. Att generella uttalanden återkommer ska snarare tolkas som att Brics-länderna inte har kunnat enas om något konkret. Rysslands internetsektor var tidig med att producera unika ryska alternativ i det

logiska lagret, men utan en stark industri på hårdvaruområdet kommer Ryssland att fortsätta att vara beroende av import av komponenter och annan teknik. Ryssland är inte i närheten av att kunna erbjuda de ekonomiska och tekniska fördelar som samarbeten med Kina innebär för Brics-länderna. Detta ryska dilemma har blivit än mer tydligt efter den fullskaliga invasionen av Ukraina 2022.

Även Indien ser Brics som instrumentellt i att höja landets status internationellt och att stärka den indiska ekonomin. Indien vill visserligen se en multipolär världsordning, men stöder inte att Brics blir en anti-västlig allians. Indien har sedan länge en konfliktfylld relation till Kina och allt starkare säkerhetspolitiska förbindelser med USA. Dessutom är Indiens tjänsteexport inom it-sfären till USA och Europa viktig för landets ekonomi. Indiska myndigheter har förbjudit flera kinesiska applikationer och företag från Kina kommer heller inte att få delta i utbyggnaden av Indiens 5G-nät.

Indien räknas inte som ett auktoritärt politiskt system, men landets ledning har visat ett ökat intresse för att samarbeta om internetsäkerhet med auktoritära länder. Kina är, trots spända relationer, Indiens största handelspartner och dominerar den indiska marknaden för smarta telefoner. I FN stöder Indien delvis Rysslands initiativ till ett informationssäkerhetsavtal och i takt med att regeringspartiet BJP (Bharatiya Janata Party) har genomfört inskränkningar i demokratin och minskat friheten på internet, har landet också närmat sig Kina och Ryssland ideologiskt på it-området.

Kina har de ekonomiska, teknologiska och industriella musklerna som krävs för att kunna driva säkerhetspolitiska mål i såväl det fysiska och logiska som i personalagret. Liksom Ryssland vill Kina kontrollera informationsflöden inom landet, men också ha en roll när globala standarder utformas. Kina delar Rysslands mål att motverka västlig dominans på det digitala området. Samtidigt är Kinas ekonomi beroende av global handel – innovation och standarder kräver interaktion med omvärlden. För Kina blir därmed Brics en av flera plattformar för att stärka kinesiskt inflytande och ledarskap på cyberområdet.

Kina tillhandahåller också en modell för auktoritära ledare vad gäller att kombinera stark kontroll över medborgarnas tillgång till information utan att isolera landet från det globala internet eller från internationell teknikutveckling. Genom att satsa på digital teknikutveckling vill Kina undvika att falla offer för yttre påtryckningar och dessutom utmana den amerikanska dominansen på området. USA:s sanktioner har troligen bidragit till att Kina kommer att sträva efter att bli självförsörjande i samtliga lager av cyberdomänen.

Sydafrikas utrikes- och säkerhetspolitik vilar på politiska ideal, som innefattar demokrati och mänskliga fri- och rättigheter, men präglas samtidigt av nära historiska band till Ryssland, Kina och i viss mån, Iran. Landets främsta politiska mål är att främja ekonomisk utveckling och i det sammanhanget kan stärkta relationer med repressiva stater spela en roll. För Sydafrika innebär Brics en möjlighet att främja landets ekonomi. Dessutom stärker medlemskapet i Brics landets globala position och har till och med inneburit något av en symbolisk ledarroll för Sydafrika på den afrikanska kontinenten. Det återstår att se hur utvidgningen till Brics+, som nu även omfattar Egypten och Etiopien, förändrar Sydafrikas ställning inom organisationen.

Sydafrika delar kritiken mot västlig dominans, men vill inte bryta banden till västliga länder. Landet importerar såväl mjuk- som hårdvara och lider brist på inhemsk expertis samtidigt som otillräcklig elförsörjning lägger hinder för den digitala utvecklingen. Därmed blir både tillgång till ny teknik för alla Brics-medlemmar och åtgärder för att minska den digitala klyftan viktiga politiska mål för Sydafrika. Landets politik framstår dock ofta som otydlig i avsaknad av en övergripande strategi för cyberområdet.

## Säkerhetspolitiska och tekniska drivkrafter

Den globala tekniska utvecklingen har lett till att cyberfrågor har blivit centrala i säkerhetspolitiken för allt fler länder. Länder som kan påverka, reglera och samarbeta på cyberområdet blir säkerhetspolitiskt starkare och kan potentiellt utnyttja andra länders beroenden. USA:s handels- och tullpolitik kombinerat med den amerikanska dominansen i internets olika lager har gjort att Brics-länderna, utifrån respektive lands förutsättningar, försöker öka sin digitala autonomi gentemot väst. I deklarationen från Brics-toppmötet den 6 juli 2025 i Rio de Janeiro betonas vikten av ”gemensamma åtgärder inom området digital infrastruktur för att säkerställa integriteten, stabiliteten i funktionen och säkerheten inom de nationella segmenten av Internet, samtidigt som internetfragmentering undviks”. Liksom i tidigare Brics-deklarationer är formuleringarna relativt allmänna och utformade så att alla länder kan skriva under. Brasilien, Indien och Sydafrika är inte primärt intresserade av att byta ett beroende mot ett annat. Snarare har de mycket att vinna på att fortsatt balansera sin utrikespolitik och sitt digitala teknikberoende mellan väst och länder som Ryssland och Kina. Ryssland och Kina enas kring en politik som syftar till att försvaga

västlig dominans. Avgörande frågor kommer att vara om Brics *rör sig från* eller *närmar sig* väst, men också huruvida inställningen till väst kan komma att splittra Brics om Kina och Ryssland driver sin linje för hårt.

Allt talar för ett närmare digitalt samarbete inom Brics, men till vilken grad länderna kan enas kring konkreta åtgärder kommer att bero dels på Brics-ländernas individuella strategiska mål, dels på omvärldsutvecklingen. De drivkrafter som initialt låg bakom att Brics bildades, och som bland annat har resulterat i en alternativ utvecklingsbank, kan mycket väl också driva på en ökad fragmentering på cyberområdet globalt. Det finns fortfarande både misstänksamhet och förbittring över hur väst fortsätter att dominera globala institutioner. USA:s centrala roll i hur internet växte fram liksom det faktum att ett fåtal amerikanska multinationella företag dominerar den globala marknaden spelar här en roll. Hur väst och inte minst USA väljer att agera kan påverka politiken i samtliga Brics-länder framöver.

Det är ännu tidigt att dra slutsatser om hur utvidgningen av Brics kan komma att påverka sammanhållningen inom organisationen. Det kan bli svårare att nå enighet kring gemensamma mål med flera länder runt bordet. Samtidigt är dock flera av de nya Brics-ländernas politik mer i linje med Rysslands och Kinas vad gäller behovet av att etablera kontroll och övervakning av internet inom respektive länder av regimsäkerhetsskäl. Om Brics till exempel etablerar mer formella institutioner på cyberområdet efter Rio-deklarationen 2025, torde det vara en utveckling värd att följa nära. Säkerhetspolitiska överväganden kommer att styra Brics-länders infrastrukturval i närtid och därmed i sin tur bestämma huruvida internets logiska och fysiska lager kommer att utvecklas mot ökad fragmentering.

# Innehåll

Sammanfattning ... vi

Brics-länderna och digitalt samarbete ... vi

Säkerhetspolitiska och tekniska drivkrafter ... vii

**1. Inledning** ... 13
*Per-Erik Nilsson och Carolina Vendil Pallin*

Syfte och forskningsfråga ... 14

Metod ... 14

Avgränsningar ... 15

Centrala begrepp ... 15

Studiens struktur ... 15

**2. Brics och internet** ... 19
*David Lindahl, Per-Erik Nilsson och Carolina Vendil Pallin*

2.1 Brics som samarbetsformat ... 19

Mellan splittring och enighet ... 19

Brics expanderar ... 20

Brics-ländernas ekonomiska styrka ... 21

Brics-samarbete på cyberområdet ... 23

Brics framtid ... 24

2.2 Vad är internet? ... 24

Paketförmedlande nätverk och dirigering ... 25

Internets dirigeringsnivåer ... 25

Internet och cyberdomänens lager ... 26

Reglering av internet ... 27

2.3 Säkerhetskonsekvenser av internets infrastruktur ... 28

Dirigering ... 28

Kabelavlyssning ... 28

Serviceavbrott ... 29

Hårdvara, produktion och leverantörskedjor ... 29

2.4 Sammanfattning ... 30

**3. Brasilien – en balanserande regional makt** ..... 35
*Olivier Milland*

3.1 Brasiliens relation till Brics ..... 35
3.2 Internets utveckling i Brasilien ..... 37
Brasiliens beroende av utländska företag ..... 39
3.3 Internets tillstånd och framtid i Brasilien ..... 41
Drivkrafter och hot som förklarar Brasiliens agerande ..... 44
Brasiliens hotbild ..... 45
3.4 Brasiliens ansats till Brics-samarbetet i cyberdomänen ..... 45
3.5 Slutsatser ..... 46

**4. Ryssland – Brics som digital hävstång** ..... 53
*Carolina Vendil Pallin*

4.1 Rysslands relation med Brics ..... 53
4.2 Internets utveckling i Ryssland ..... 54
4.3 Rysslands cyberinfrastruktur ..... 54
Internetknutpunkter och sjökablar ..... 55
Ett suveränt internet ..... 56
Rysk it-industri ..... 57
4.4 Ryska initiativ inom Brics på cyberområdet ..... 59
Inom Brics ..... 59
Ett internationellt FN-avtal ..... 60
4.5 Slutsatser ..... 61

**5. Indien – ”Ickevästlig men inte antivästlig”** ..... 67
*Samuel Neuman Bergenwall*

5.1 Indiens relation med Brics ..... 67
5.2 Internets utveckling i Indien ..... 68
5.3 Internets samtida tillstånd i Indien ..... 70
Indisk it-tjänsteexport ..... 71
Indisk lagstiftning och nationell suveränitet ..... 71
Frihet, övervakning och informationsoperationer på internet ..... 72
5.4 Brics och Indiens ambitioner på internetområdet ..... 74
5.5 Slutsatser ..... 75

**6. Kina – cyberstormakten i Brics** ..... 81
*Per-Erik Nilsson*

6.1 Kinas relation med Brics ..... 81
6.2 Internets utveckling i Kina ..... 81
6.3 Internet i dag i Kina ..... 84
6.4 Kina, säkerhetspolitik och Brics ..... 87
Kinas cyberpolitik och internationell säkerhet ..... 87
Kinas cyberpolitik och Brics ..... 89
6.5 Slutsatser ..... 90

**7. Sydafrika – en passiv och ambivalent vågmästarstat** ..... 99
*Anna Ida Rock*

7.1 Sydafrikas relation med Brics ..... 99
7.2 Internets utveckling i Sydafrika ..... 100
It för utveckling och den digitala klyftan ..... 100
Öppenhet och frihet på internet ..... 101
Cybersäkerhet ..... 102
7.3 Internets samtida tillstånd i Sydafrika ..... 103
Begränsningar och beroenden ..... 104
7.4 Brics och Sydafrikas ambitioner på internetområdet ..... 105
7.5 Slutsatser ..... 106

**8. Slutsatser – Brics framtida digitala samarbete** ..... 113
*Per-Erik Nilsson och Carolina Vendil Pallin*

8.1 Geopolitiska och säkerhetspolitiska drivkrafter ..... 113
8.2 Inrikespolitiska drivkrafter ..... 114
8.3 Teknisk och teknologisk utveckling som drivkraft ..... 115
8.4 Framåtblick ..... 116
8.5 Vidare forskning ..... 117

## Figurer

**Figur 2.1** Storlek på BNP i löpande priser för Brics-länderna, EU och USA 1990–2025. 22
**Figur 2.2** BNP för Brics-länderna, EU och USA i köpkraftsparitet 1990–2025. 22
**Figur 2.3** BNP-tillväxt för Brics-länderna och USA 1990–2025. 22
**Figur 2.4** Brics-kabelns planerade sträckning. 24
**Figur 2.5** Internets dirigeringsnivåer. 26
**Figur 2.6** Cyberdomänens lager. Modell hämtad från Försvarsmakten, ”Doktrininsats: Cyberförsvar”, DA CYBER 2024, Versionsnr. 1.1. 26
**Figur 2.7** Undervattenskabelkarta, Submarine Cable Map (Creative Commons License: CC BY-SA 4.0). 29
**Figur 3.1** Författarens anpassning av data om Brasiliens internationella internetkablar och datacenter från TeleGeography – The Submarine Cable Map och Data Center Map. 38
**Figur 3.2** Brasiliens marknad för 5G mobiltelefoni, 2021-24. 39
**Figur 4.1** Befintliga och planerade sjökablar som ansluter till ryskt territorium. 55

## Tabeller

**Tabell 2.1** Befolkningsmängd i Brics (efter 2023) enligt siffror från Världsbanken 2023 20
**Tabell 2.2** Ordförandeland och toppmöten 2009–2025. 21
**Tabell 8.1** Schematisk beskrivning av Bricsländernas position inom cyberområdet. 114

# 1. Inledning

*Per-Erik Nilsson och Carolina Vendil Pallin*

*Föreställ er ”deras” internet – västligt, med all världens smörja, utsvävningar och lort. Och så borde vårt finnas. Ett internet där traditionella värden och godhet härskar. En cybermiljö med sina regler och lagar. Cyberpolis och cyberarmé för att försvara mot yttre hot.*

Ledamot, i ryska parlamentets underhus (Duman), 2023[1]

Ryssland har sedan 2015 varit drivande inom Brics för att ”avmonopolisera” internet. Vid den tiden kritiserades särskilt den amerikanska relationen till organisationerna *Internet Corporation for Assigned Names and Numbers* (ICANN) och *Internet Assigned Numbers Authority* (IANA) som reglerar internets styrning, policy, samordning och tekniska grunder.[2] 2016 klipptes dock de officiella banden mellan amerikanskt överseende och organisationerna som idag är självständiga och icke-vinstdrivande globala organisationer.[3] Som diskuteras nedan är det ryska säkerhetstänkandet inte obefogat men, som citatet ovan antyder, handlar Rysslands tänkande på området inte primärt om att skydda sig tekniskt från intrång som spionage, brottslighet och sabotage, utan snarare om ett internet fritt från västerländska värderingar och ideologi.

Anledningarna till att internet har kommit att få en alltmer framträdande plats på Brics-ländernas säkerhetspolitiska agenda är flera.[4] Edward Snowdens avslöjanden om hur USA kunnat utnyttja sitt försprång och inflytande för att avlyssna internettrafik 2013 beskrivs inom forskningen ha accelererat enskilda Brics-länders strävan att skydda sin informationssfär men också samarbetet inom området länderna emellan. En minst lika viktig drivkraft för vissa av Brics-länderna, främst Kina och Ryssland, förefaller ha varit att öka kontrollen över informationsspridning inom sina respektive länder. För Kina var protesterna för demokrati i Hongkong en larmklocka om vilka faror som fri information kunde innebära för landets kommunistiska och auktoritära system. För Ryssland blev redan tidigare protesterna i Moskva och resten av landet 2011–2012 startskottet för ett systematiskt arbete med att minska friheten på internet. För båda länderna var även den arabiska våren 2011 en varningsklocka. Sociala medier och internet som helhet framstod för dessa båda auktoritära länder som ett hot värt att ta på yttersta allvar. Även i Brasilien har myndigheternas kontroll över vilken information landets internetanvändare har tillgång till blivit en central säkerhetspolitisk fråga de senaste åren, men från en något annorlunda ansats än Rysslands och Kinas. I Brasilien har spridningen av desinformation och hotet det medför mot den brasilianska demokratin varit en central faktor. För Indien och Sydafrika har behovet att kontrollera vilken information landets medborgare får ta del av inte uttryckligen varit en lika stark drivkraft som för de andra tre länderna (för Indien har dock behovet ökat om än inte till samma nivå som i Kina och Ryssland). Däremot verkar argumentet att minska västs inflytande på cyberområdet i viss mån ha förenat länderna i frågor om internets framtid liksom även ett mål att få ta del av utvecklingen inom informationsteknik, från fysisk infrastruktur till mjukvara och artificiell intelligens (AI). För Sydafrika, Indien och Brasilien innebär det dock inte att man vill bryta sina relationer på det digitala området med väst.

Ett separat Brics-internet skulle kunna ses som ett tydligt tecken på att Brics-länderna inte bara distanserar sig från västländer, utan vänder sig mot dem. I takt med att Brics har vuxit från fem medlemmar (Brasilien, Ryssland, Indien, Kina och Sydafrika) till elva (Saudiarabien, Egypten, Förenade Arabemiraten, Etiopien, Indonesien och Iran) framstår det dock som att frågan om ett separat internet åtminstone tillfälligt har fått stå tillbaka. I den senaste deklarationen efter Brics-ländernas årliga toppmöte behandlades internet i endast en av 126 paragrafer: ”Vi uppmuntrar Brics-medlemmarna att undersöka möjligheten till

1 ”V Gosdume predlozjili Mintsifry sozdat jedinyj internet so stranami BRIKS+”, *RIA Novosti*, 12 maj 2023.

2 Igor Agapov, ”Rossija rasstjityvajet na BRIKS v demonopolizatsii Interneta”, *Comnews*, 28 april, 2015.

3 ICANN, ”Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends”, 1 oktober 2016.

4 Luca Belli, red., *CyberBRICS: Cybersecurity Regulations in the BRICS Countries* (Cham: Springer, 2021).

gemensamma åtgärder inom området digital infrastruktur för att säkerställa integriteten, stabiliteten i funktionen och säkerheten hos de nationella segmenten av internet, samtidigt som internetfragmentering undviks".[5] Trots detta är internet troligen en fortsatt viktigt säkerhetspolitisk fråga för framtiden och enskilda Brics-länder fortsätter att driva initiativ för att förändra reglering och styrning av det globala internet.

## Syfte och forskningsfråga

Västerländska analytiker och forskare har under ett drygt decennium diskuterat huruvida Brics-länderna söker skapa ett regionalt internet. Den trots detta relativt knapphändiga tidigare forskningen om Brics och internet refereras återkommande i rapporten. Forskaren Marek Rewizorski har delat in forskningen om Brics i tre debatter. Den första debatten handlar om Brics roll som ett framväxande multilateralt maktorgan och dess potential att omforma den globala världsordningen och etablera nya former av global styrning. Den andra debatten fokuserar på Brics bidrag till global ekonomisk styrning. Här lyfts också konflikter mellan Brics medlemmar fram, som konkurrensen mellan Indien och Kina, samt hur dessa påverkar organisationens effektivitet. Den tredje debatten undersöker Brics interna samordning och hur dess toppmöten påverkar medlemmarnas inrikespolitiska prioriteringar och mål.[6] *Föreliggande rapport* bidrar i viss mån till samtliga dessa spår; den behandlar Brics samarbetsorgan, de spänningar som finns mellan länderna inom Brics samt kopplingen mellan inrikes- och utrikespolitiska mål, men med ett fokus på internet och säkerhetspolitik.

Ett separat Brics-internet skulle, om det realiserades, sannolikt innebära att en stor del av världens internetanvändare befinner sig i en cyberrymd som definieras av lagar, ekonomiska villkor samt teknisk infrastruktur och lösningar som skiljer sig alltmer från de som västliga internetanvändare möter framför skärmen. Ett Brics-internet skulle sannolikt även innebära förändrade villkor för internationella, sociala, inrikespolitiska och ekonomiska relationer. Säkerhetspolitiskt skulle en utveckling i den här riktningen sannolikt skapa större splittring mellan världens ekonomiska och militära stormakter samt vara en viktig variabel i en multipolär världsordning.

Mot denna bakgrund är syftet med rapporten att skapa en djupare förståelse, inte bara för den här eventuella utvecklingen, men även för hur de drivande länderna ser på en sådan utveckling i en tid när internet och annan informations- och kommunikationsteknik blir en alltmer central del av alla aspekter av mänskligt liv.

Rapportens övergripande forskningsfråga är således:

- I vilken utsträckning driver de ursprungliga Brics-länderna en gemensam agenda för att skapa ett framtida och separat Brics-internet?

För att besvara frågan diskuterar den här rapporten de ursprungliga och enskilda Brics-ländernas relation till och förståelse av internet- och säkerhetspolitik. För varje land har den övergripande forskningsfrågan delats upp i delfrågor som ställs om respektive land:

- Vilka infrastrukturella val rörande internet och annan it har gjorts?
- Hur har dessa val förklarats och motiverats?
- Vilken uttryckt roll spelar säkerhetspolitik i valen?
- Vilken roll spelar landet i relation till en gemensam internetpolitisk hållning i Brics?
- Vilka, om några, enskilda initiativ i relation till styrning och reglering av internet drivs?

Svaren på dessa frågor diskuteras sedan i relation till potentiella säkerhetspolitiska konsekvenser.

Rapporten riktar sig främst till analytiker och praktiker som arbetar med de frågor som berörs av rapporten, men även den intresserade läsaren. Varje kapitel är skrivet så att de kan läsas separat, men givet ambitionen att nå även en bred läsekrets, innehåller rapporten grundläggande aspekter av internets funktion, reglering och styrning samt om Brics som organisation (kapitel 2) som hjälper den obevandrade läsaren i just dessa frågor att navigera de specifika kapitlen.

## Metod

Ansatsen i rapporten är explorativ och tvärvetenskaplig. Ett syfte med rapporten har varit att, föra samman FOI:s säkerhetspolitiska regionbaserade forskning med forskning om internet och cybersäkerhet. Rapportens

5 "Rio de Janero Declaration", Brics, 6 juli 2025.

6 Marek Rewizorski, "Brics and New Multilateral Development Banks: Towards Recalibration of Global Economic Governance", *Przegląd Strategiczny*, nr. 11 (2018): 281–98.

källmaterial bygger till stor del på tidigare forskning och analys samt nyhetsrapportering och officiella uttalanden från de analyserade aktörerna. Urvalet av material har skett dels via sökningar i forskningsdatabaser (t.ex. Scopus och Web of Science) och den så kallade snöbollsmetoden (där en källa leder vidare till flera) samt författarnas tidigare förkunskaper. Rapporten är också tänkt att kunna ligga som grund för framtida, systematiska jämförande studier på området.

Arbetet med rapporten initierades med ett seminarium hösten 2024 där centrala frågor och begrepp diskuterades. Detta har efterföljts av författarnas självständiga forskning och skrivande, uppföljande seminarier, läsande av varandras texter och med en granskning av forskare med områdesexpertis.

## Avgränsningar

Rapporten fokuserar i huvudsak på internets infrastruktur (det så kallade fysiska lagret). Detta utesluter dock inte att frågor om ekonomi, politik, industri samt AI och mjukvara (det så kallade logiska lagret) berörs. Vilka aspekter som diskuteras beror på tillgängliga källor samt på de enskilda ländernas specifika utveckling och hållning i frågor som rör internets framtid, generellt och vad gäller ett eventuellt Brics-internet. En strikt jämförelse mellan länderna skulle kräva mer djuplodande empirisk forskning som inte har varit möjlig inom tidsramen för arbetet med denna rapport.

## Centrala begrepp

För att nyansera delfrågorna är det viktigt att undersöka vad ett Brics som samarbetar för att öka sitt inflytande över internet skulle innebära i tekniska och legala termer. Här ryms en rad besläktade koncept. Två centrala begrepp för den här rapporten är ”internetfragmentering” och prefixet ”cyber”.

Internetfragmentering (även kallat *splinternet*) brukar användas som samlingsterm för olika scenarier där det globala internet delas upp i olika zoner där användare inte längre har tillgång till hela internet utan endast en geografisk eller tekniskt definierad zon.[7]

I den här rapporten görs en skillnad mellan teknisk fragmentering av internet, som alltid har förekommit, och en politiskt driven uppdelning av internet. Internet, som i sig är ett nätverk av nätverk, är redan idag tekniskt fragmenterat så till vida att alla nätverk inte är tillgängliga för alla. Ett exempel på det senare är intranät som är avskärmade från det globala internet. Inom forskningen talas det även om ”galapagossyndromet” när tekniska lösningar blir för lokalt anpassade så att de blir inkompatibla med globala system.[8] Andra exempel är tjänster och nätverk som är låsta till en särskild hård- och mjukvara. Apple, Google och Microsoft har ekosystem av hårdvara och mjukvara som präglas av ekosystem-låsning (*vendor-lock-in*), eftersom de designar sina produkter för att fungera bäst inom sina egna system och ibland begränsar kompatibiliteten med konkurrenternas lösningar. Dessutom kan tekniska missöden innebära att internet drabbas av en tillfällig fragmentering.

Den politiskt drivna fragmenteringen av internet (*internet alignment*) beskrivs i forskningen ofta som ”balkanisering”, och innebär att statliga aktörer försöker öka sitt inflytande över en geografiskt definierad del av internet. Om allt fler regeringar, antingen genom lagstiftning eller genom tekniska lösningar som inte är kompatibla med globala standarder, försöker kontrollera kommunikationen inom ett visst territorium riskerar det att begränsa internet som en global kommunikationssfär.

Angående ”cyber” består internet inte endast av teknisk infrastruktur och digital kommunikation. Mjukvara och mänskliga användare av internet är minst lika viktiga. I rapporten används ”cyber” som ett övergripande prefix för att beskriva områden relaterade till digitala data, digital kommunikation och nätverk (inklusive internet) och it-infrastruktur. I detta sammanhang omfattar ”cyberdomänen” både de tekniska system som möjliggör att skapa digital information, de tekniker som används för att hantera, lagra och överföra den, och människorna som använder sig av detta.

## Studiens struktur

Detta inledande kapitel har syftat till att presentera studiens syfte och upplägg. Kapitel två beskriver Brics bildande och utveckling samt ger en teknisk bakgrund

7 Rapporten utgår särskilt från Milton L. Muellers forskning om internet och fragmentering, se: Milton L. Mueller, *Will the Internet Fragment?* (Cambridge: Polity, 2017), 29–31. Se även Konstantinos Komaitis, ”Internet Fragmentation: Why It Matters”, EU Cyber Direct – Research in Focus, januari 2023; Milton L. Mueller, “Against Sovereignty in Cyberspace”, *International Studies Review*, vol. 22, nr. 4 (2020): 779–801; Dana Polatin-Reuben och Joss Wright, ”An Internet with BRICS Characteristics”, *4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14)*, San Diego, CA, 7 juli 2014: 1–10.

8 Mary Reisel, ”From Galapagos Syndrome” to Globalization: Japanese Business Between Tradition and Virtual Reality”, *International Journal of Business Anthropology,* vol. 7, nr. 2 (2017): 1–21.

om internet. Därefter följer fem kapitel som i bokstavsordning (Brics – Brasilien, Ryssland, Indien, Kina respektive Sydafrika) behandlar rapportens forskningsfrågor i relation till respektive land. Kapitel åtta avslutar rapporten med en syntes av samtliga kapitel. Syntesen utvärderar möjligheterna till samarbete på internetområdet, uppdelat i geopolitiska, inrikespolitiska samt tekniska och teknologiska drivkrafter. Kapitlet avslutas med ett framåtblickande resonerande avsnitt och förslag på vidare forskning.

# Referenser

”Rio de Janeiro Declaration”. Brics. 6 juli 2025, hämtad 5 oktober 2025. *http://brics.br/en/documents/presidency-documents/250705-brics-leaders-declaration-en.pdf*.

”V Gosdume predlozjili Mintsifry sozdat jedinyj internet so stranami BRIKS+”. *RIA Novosti*, 12 maj 2023, hämtad 5 oktober 2025. *https://ria.ru/20231110/internet-1908609747.html*.

Agapov, Igor. ”Rossija rasstjityvajet na BRIKS v demonopolizatsii Interneta”. *Comnews*, 28 april 2015, hämtad 5 oktober 2025, *https://www.comnews.ru/content/91391/2015-04-28/rossiya-rasschityvaet-na-briks-v-demonopolizacii-interneta*.

Belli, Luca, red. *CyberBRICS: Cybersecurity Regulations in the BRICS Countries*. Cham: Springer, 2021.

ICANN. ”Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends”. 1 oktober 2016, hämtad 5 oktober 2025. *https://www.icann.org/en/announcements/details/stewardship-of-iana-functions-transitions-to-global-internet-community-as-contract-with-us-government-ends-1-10-2016-en*.

Komaitis, Konstantinos. ”Internet Fragmentation: Why It Matters”. *EU Cyber Direct – Research in Focus*. januari 2023, hämtad 5 oktober 2025, *https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/ioyLip9O/internet-fragmentation-why-it-matters-for-europe.pdf*.

Mueller, Milton L. *Will the Internet Fragment?* Cambridge: Polity, 2017.

Mueller, Milton L. ”Against Sovereignty in Cyberspace”. *International Studies Review*, vol. 22, nr. 4 (2020): 779–801.

Polatin-Reuben, Dana och Joss Wright. ”An Internet with BRICS Characteristics”. *4th USENIX Workshop on Free and Open Communications on the Internet* (FOCI 14), San Diego, CA, 7 juli 2014: 1–10.

Reisel, Mary. ”From “Galapagos Syndrome” to Globalization: Japanese Business Between Tradition and Virtual Reality”. *International Journal of Business Anthropology*, vol. 7, nr. 2 (2017): 1–21.

Rewizorski, Marek. ”Brics and New Multilateral Development Banks: Towards Recalibration of Global Economic Governance”. *Przegląd Strategiczny*, nr. 11 (2018): 281–98.

# 2. Brics och internet

*David Lindahl, Per-Erik Nilsson och Carolina Vendil Pallin*

Detta kapitel inleder med att beskriva hur Brics bildades och ger en allmän bakgrund om organisationen i termer av befolkning och ekonomisk styrka hos de olika länderna. Kapitlet ger även en bakgrundskunskap om den tekniska infrastruktur som ligger till grund för dagens internet, förmedlar kort hur internet är uppbyggt och vad säkerhetskonsekvenserna blir av att det är uppbyggt på detta specifika sätt. Kapitlet ska bidra till att läsaren kan följa resonemang och slutsatser som presenteras i de övriga kapitlen.

## 2.1 Brics som samarbetsformat

Termen ”Bric” kommer från en rapport från investmentbanken Goldman Sachs.[1] Rapporten beskrev en investeringsstrategi baserad på länder som hade en stark tillväxt: Brasilien, Ryssland, Indien och Kina (Bric).[2] Denna akronyms färd ur investment-banking-världen in i storpolitiken skedde på ryskt initiativ. Redan 2006 höll dessa länder ett möte i marginalen av FN:s generalförsamlings (UNGA) session. Från Ryssland, Indien och Kina deltog utrikesministrarna – från Brasilien, försvarsministern. Länderna fortsatte att träffas i Bric-formatet, t.ex. i samband med G20- och G8-möten innan det första formella toppmötet ägde rum, återigen på ryskt initiativ, i Jekaterinburg i juni 2009. Därmed var Bric etablerat med ett roterande ordförandeskap och årliga toppmöten. Sydafrika blev medlem i december 2010 och från och med 2011 blev formatet därmed Brics (med ett tillagt ”s” för Sydafrika). När Sydafrika för första gången stod värd för det årliga Brics-mötet 2013, deklarerade den sydafrikanske presidenten Jacob Zuma att Brics nu hade etablerats ”som en trovärdig och konstruktiv grupp i vår strävan att forma ett nytt paradigm för globala relationer och samarbete”.[3]

### Mellan splittring och enighet

Sedan Brics skapande har akademiker och analytiker diskuterat hur organisationen skulle kunna omforma strukturer för globalt styrande och samarbete.[4] I Europa och USA har många kritiserat Brics både som projekt och som en analytisk kategori, eftersom skillnaderna mellan länderna ansågs vara större än deras gemensamma nämnare.[5] Andra skeptiska röster kallade exempelvis Brics år 2013 för ”upphaussat” och ”en artificiell konstruktion” som under en överskådlig framtid inte kommer att bli mycket mer ”än en akronym skapad av en amerikansk bankir”.[6] I en analys av Brics-ländernas koordinering i G20 påvisar en studie att den åtminstone fram till 2019 har varit bristfällig och att nationella intressen har vunnit över gemensamma.[7]

I en annan studie om Brics-ländernas röstande i UNGA framgår att länderna fram till 2014 inte var samstämmiga, särskilt inte vad det gäller frågor om dödsstraff, mänskliga rättigheter och icke-spridning av kärnvapen.[8] Just frågan om mänskliga rättigheter lyfts i den tidigare forskningen som en vattendelare mellan å ena sidan Kina och Ryssland, å den andra Brasilien, Indien, Sydafrika.[9] Mot denna bakgrund skriver exempelvis

1 Jim O’Neill, *Building Better Global Economic BRICs*, Goldman Sachs, Global Economics Paper. nr. 66, 2001.
2 Bokstaven ”c” i Bric hänvisar till den engelska benämningen av Kina (*China*).
3 Jacob Zuma, ”Durban Summit: Plenary Address”, BRICS Information Centre, Toronto University, 27 mars 2013.
4 Niall Duggan et al, ”Introduction: ’The BRICS, Global Governance, and Challenges for South–South Cooperation in a Post-Western World’”, *International Political Science Review*, vol. 43, nr. 4 (2022): 469–80, 470.
5 Se: Oliver Stuenkel, *The BRICS and the Future of Global Order* (Lanham, Boulder, New York och London: Lexington Books, 2020), 1.
6 Se t.ex. Harsch V. Pant, ”The BRICS Fallacy”, *The Washington Quarterly*, vol. 36, nr. 3 (2013): 91–105, 103.
7 Niall Duggan och Juan Carlos Ladines Azalia, ”From Yekaterinburg to Brasilia: BRICS and the G20, Road to Nowhere?” *Revista Brasileira de Política Internacional*, vol. 63, nr. 1 (2020): e009, 10.
8 Bas Hooijmaaijers och Stephan Keukeleire, ”Voting Cohesion of the BRICS Countries in the UN General Assembly, 2006−2014: A BRICS Too Far?” *Global Governance: A Review of Multilateralism and International Organizations*, vol. 22, nr. 3 (2016): 389–408, 403–404.
9 Aleksandr Ignatov, ”The BRICS Agenda on the Internet Governance”, *International Organisations Research Journal*, vol. 17, nr. 2 (2022): 86–109.

Stewart Patrick att Brics kommer att vara ”en arena för framväxande och regionala makter att främja sina (ibland) överlappande intressen”.[10]

Forskare och analytiker från Brics-länderna tenderar att vara mer positiva och se fördelar med formatet samt kritisera västlig analys för etnocentrism.[11] Brics-formatet har onekligen visat sig mer livskraftigt än många västliga kommentatorer förutspått.[12] En tydlig framgång var etablerandet 2015 av Nya utvecklingsbanken (The New Development Bank) och Reservfonden (Contingent Reserve Arrangement).[13] Tillsammans utmanar dessa organ det som brukar beskrivas som ”the Washington Consensus”, det vill säga principerna som har varit vägledande när Världsbanken och Internationella valutafonden (International Monetary Fund, IMF) stöder utvecklingsländer. Dessa västliga principer innebär att marknadsekonomiska överväganden som frihandel, privatisering och åtgärder för att minska inflation och budgetunderskott ska åtföljа ekonomiskt stöd. Om Nya utvecklingsbanken och Reservfonden lyckas att etablera sig som stöd till utvecklingsprojekt i det globala syd kommer det sannolikt att stärka Brics legitimitet.[14]

## Brics expanderar

Vilka länder som ska ingå i samarbetet har varit omtvistat. De mer västligt orienterade medlemmarna har exempelvis uttryckt missnöje med inkluderandet av Iran i Brics. I Johannesburg 2023 tog Bricsländerna detta till trots beslutet att utvidga formatet genom att bjuda in Argentina, Egypten, Etiopien, Förenade Arabemiraten, Iran och Saudiarabien. Alla länder anslöt under 2024, utom Argentina som efter ett skifte på presidentposten valde att dra tillbaka sin Bricsansökan. I stället för Argentina valde dock Indonesien att ansluta till samarbetet. Saudiarabien stod som Bricsmedlem på Brasiliens Brics-webbsida 2025, men har formellt inte deklarerat att landet har blivit medlem, troligen för att inte störa relationerna med USA.[15] Brics omfattar därmed fler än tre och en halv miljard människor av jordens åtta miljarder (se Tabell 2.1).

**Tabell 2.1** Befolkningsmängd i Brics (efter 2023) enligt siffror från Världsbanken 2023 (avrundade till jämna hundratusental)[(1)]

| Brics-land | Antal invånare (tusental) |
|---|---|
| Brasilien | 211 998 |
| Egypten | 116 538 |
| Etiopien | 123 060 |
| Förenade Arabemiraten | 10 877 |
| Indien | 1 450 936 |
| Indonesien | 283 488 |
| Iran | 91 568 |
| Kina | 1 408 975 |
| Ryssland | 143 534 |
| Saudiarabien (se anm.) | 35 300 |
| Sydafrika | 67 007 |
| **Totalt** | **3 943 281** |

**Anm:** Saudiarabien deltar i Brics-möten och listas som medlem på Brics-hemsidan under Brasiliens ordförandeskap 2025 (https://brics.br/en/about-the-brics), men hade inte formellt deklarerat att landet är medlem i Brics 2025.

**Källa:** Världsbanken, ”Population, total”, 2 oktober 2024.

Från och med den 1 januari 2024 omfattade således Brics tio medlemsländer (eller möjligen elva beroende på Saudiarabiens medlemskap), men saknade fortfarande ett högkvarter med tillhörande byråkrati och en huvudstad för organisationen. Ett roterande ordförandeskap och årliga toppmöten utgjorde fortfarande kärnan i samarbetet. Under 2024 stod Ryssland för ordförandeskapet (se Tabell 2) med devisen ”Stärkande av multilateralism för en rättvis global utveckling och säkerhet”.[16]

Att ytterligare utvidga Brics var också förenat med ett dilemma – i takt med att fler länder ingår riskerar flera av de ursprungliga grundarländernas makt att minska inom organisationen. Kina kommer att vara fortsatt starkt i kraft av sin ekonomiska och befolkningsstorlek,

10 Stewart Patrick, ”BRICS Expansion, the G20, and the Future of World Order”, *Carnegie Endowment for International Peace*, 9 oktober 2024.

11 Se exempelvis: Tianjiao Jiang, ”The Shift of China’s Strategic Thinking on Cyberwarfare Since the 1990s”, *Journal of Chinese Political Science*, vol. 28, nr. 1 (2023): 127–49.

12 I rapporten används begreppen ”väst” och ”globala syd”. Väst avser i första hand EU, USA och andra OECD-demokratier. Globala syd används i bred bemärkelse för länder utanför väst och betecknar G77 och postkoloniala länder i Afrika, Asien och Sydamerika. Det bör understrykas att begreppen inrymmer en betydande heterogenitet men används i rapporten för att på en högst generaliserande nivå identifiera ekonomiska, politiska och geografiska regioner i världen. Se vidare: ”Global North and Global South”, Britannica, 29 augusti 2025.

13 Duggan m.fl., ”Introduction: ’The BRICS, Global Governance”, 473.

14 G. Venkat Raman och Rajan Kumar, ”Introduction”, i *Locating BRICS in the Global Order*, red. Rajan Kumar, Meeta Keswani Mehra, G. Venkat Raman och Meenakshi Sundriyal (London and New York: Routledge, 2023, 1–14, 11.

15 Pesha Magid, Maha El Dahan och Manya Saini, ”Saudi Arabia sits on fence over BRICS with eye on vital ties with US”, *Reuters*, 8 maj 2025.

16 Kreml, ”Obrasjtjenije Vladimira Putina v svjazi s natjalom predsedatelstva Rossii v BRIKS”, 1 januari 2024.

**Tabell 2.2** Ordförandeland och toppmöten 2009–2025.

| År | Ordförandeland | Toppmöte | Anm. |
|---|---|---|---|
| 2006 | - | | Bricländernas utrikesministrar träffas i samband med UNGA:s årliga session på ryskt initiativ. |
| 2009 | Ryssland | Jekaterinburg | |
| 2010 | Brasilien | Brasilia | |
| 2011 | Kina | Sanja | |
| 2012 | Indien | New Delhi | |
| 2013 | Sydafrika | Durban | |
| 2014 | Brasilien | Fortaleza | |
| 2015 | Ryssland | Ufa | Ryskt initiativ på internetområdet. |
| 2016 | Indien | Benaulim | |
| 2017 | Kina | Xiamen | |
| 2018 | Sydafrika | Johannesburg | |
| 2019 | Brasilien | Brasilia | |
| 2020 | Ryssland | St Petersburg | Covid – videokonferens |
| 2021 | Indien | New Delhi | Covid – videokonferens |
| 2022 | Kina | Beijing | Videokonferens |
| 2023 | Sydafrika | Johannesburg | Argentina, Egypten, Etiopien, Förenade arabemiratet, Iran och Saudiarabien inbjöds att delta (Argentina valde att avstå) |
| 2024 | Ryssland | Kazan | Egypten, Etiopien, Förenade arabemiratet och Iran ansluter. Oklar status för Saudiarabien. |
| 2025 | Brasilien | Rio de Janero | Indonesien ansluter. |

liksom möjligen Indien. Men för Brasilien, Ryssland och Sydafrika innebär fler medlemmar troligen mindre relativt inflytande, i synnerhet om Brics ska fortsätta att leva upp till den egna devisen om att erbjuda samarbete på mer rättvisa villkor än väst. Sydafrikas förslag om att bara bjuda in nya medlemmar som inte skulle ha samma status som de ursprungliga Brics-länderna understryker snarare än löser dilemmat.[17]

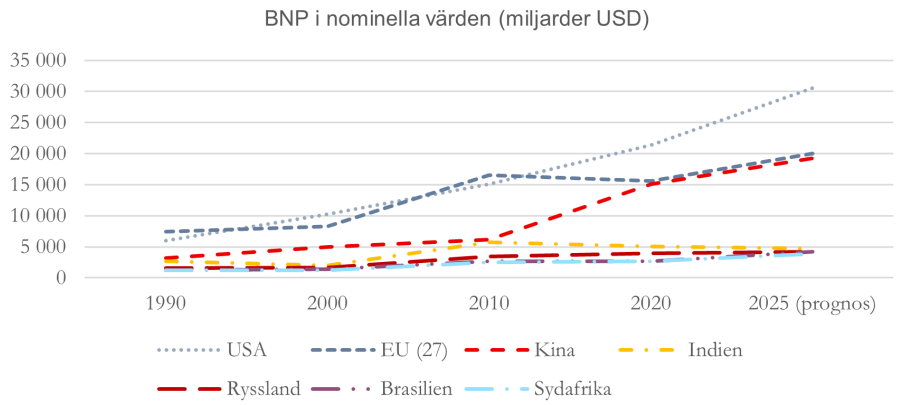
## Brics-ländernas ekonomiska styrka

Ett viktigt argument för samarbetet har varit att Bricsländernas samlade ekonomiska styrka borde ge dem större inflytande att påverka den internationella ordningen – att de ska ingå i gruppen ”regelmakare” (*rule-makers*), inte vara ”regeltagare” (*rule-takers*).[18] Prognoserna för när Brics-ländernas sammanlagda bruttonationalprodukt (BNP) ska överträffa exempelvis G7-ländernas har varierat, och beräkningarna påverkas av faktorer som huruvida BNP justeras för köpkraft eller inte. Det är också tydligt att det är Kina som är den viktigaste ekonomin för att det alls ska ske (se Figur 2.1 och Figur 2.2 som jämför Brics-ländernas BNP med EU:s och USA:s). Inom Brics är Kina en större ekonomi än samtliga övriga länders ekonomier sammanlagt och därmed är Pekings röst också ofta tongivande. För flera länder är medlemskapet i Brics viktigt framför allt för att få träffa Kinas politiska ledning och attrahera kinesiska investeringar.[19]

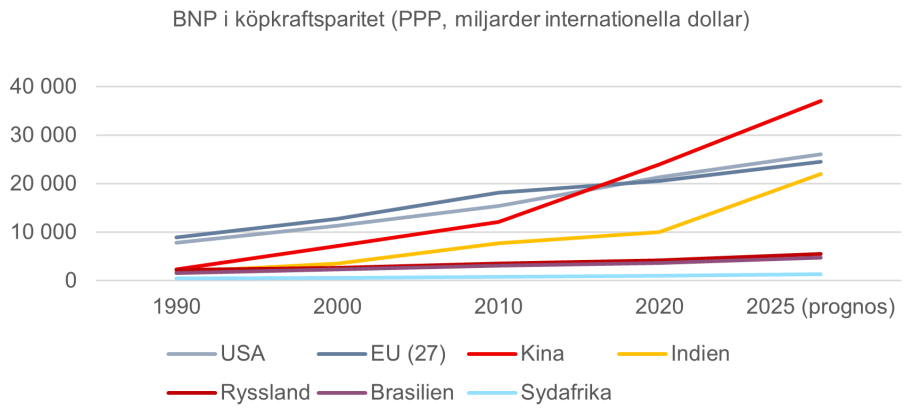
Kina har haft starkast tillväxt de senaste två decennierna, men Indien har gått om i tillväxttakt de senaste åren, medan Sydafrikas, Brasiliens och Rysslands tillväxttakt har saktat av (i Rysslands fall är tillväxten sedan 2022 primärt beroende av växande försvarsutgifter) (se Figur 2.3).

Kina har således en ledande roll inom Brics i kraft av sin ekonomiska och teknologiska styrkeposition.[20]

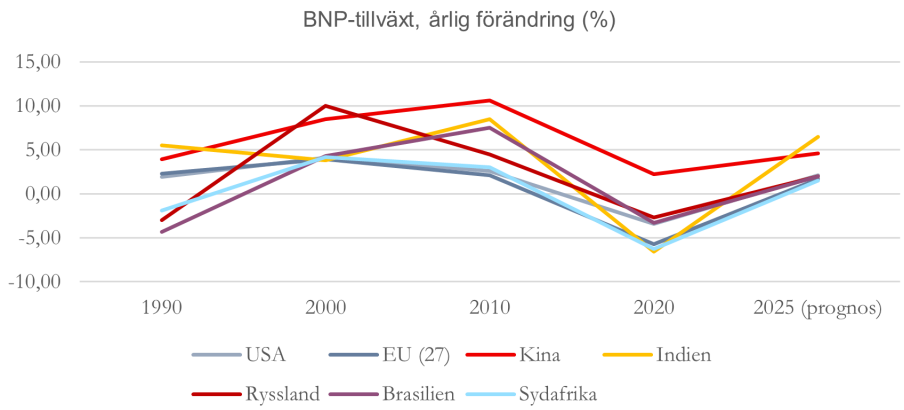
17 Sergej Strokan, ”Planeta BRIKS”, *Kommersant*, 27 december 2024.
18 Cynthia Roberts, ”Polity Forum: Challengers or Stakeholders? BRICs and the Liberal World Order”, *Polity*, vol. 42, nr. 1 (2010): 1–13, 8.
19 Alexander Gabuev och Oliver Stuenkel, ”The Battle for the BRICS: Why the Future of the Bloc Will Shape Global Order”, *Foreign Affairs*, 24 september 2024.
20 Om Kina och Brics, se: Bas Hooijmaaijers, ”China, the BRICS, and the Limitations of Reshaping Global Economic Governance”, *The Pacific Review*, vol. 34, nr. 1 (2021): 29–55.




**Figur 2.1** Storlek på BNP i löpande priser för Brics-länderna, EU och USA 1990–2025 (prognos för 2025).
**Källa:** World Economic Outlook Database.




**Figur 2.2** BNP för Brics-länderna, EU och USA i köpkraftsparitet 1990–2025 (prognos för 2025).
**Källa:** World Economic Outlook Database.




**Figur 2.3** BNP-tillväxt för Brics-länderna och USA 1990–2025 (prognos för 2025).
**Källa:** World Economic Outlook Database.

## Brics-samarbete på cyberområdet

Även om Brics-länderna kan samarbeta om en rad frågor så är det också tydligt att flera av dem vill fortsätta att vara involverade både i Brics och i den liberala internationella ordning som väst traditionellt har företrätt. De väljer även efter Rysslands invasion av Ukraina 2022 en tudelad strategi.[21]

Många forskare och analytiker framhåller att USA och Kina befinner sig i en teknisk och teknologisk kapplöpning, som enligt vissa kan leda till ett ”kallt teknikkrig” med en ”digital järnridå”, där inkompatibla tekniska standarder, internetprotokoll och infrastrukturlösningar tvingar länder till att välja sida.[22] Redan i dag existerar en rad intressanta initiativ från enskilda Brics-länder som kan ses i ljuset av denna kapplöpning.

För det första har Ryssland sedan länge drivit på för ett internationellt, juridiskt bindande, avtal om informationssäkerhet framför allt inom FN:s ram. I grund och botten handlar det om att centralisera reglering och standardisering av internet från dagens västligt dominerade flerpartsstyrningssystem (*multistakeholder approach*), som utgörs av en mångfald av tusentals aktörer, till ett system styrt av stater (se vidare 2.2.4).[23] Det sker främst inom ramen för två arbetsgrupper där Ryssland och väst hamnat i olika läger. Ryssland har dock lyckats få stöd från en rad länder för sina initiativ i FN:s generalförsamling bland annat från Brics-länderna.[24] I ett tidigt skede försökte även Ryssland ge sken av att Brasilien och Indien stödde ett ryskt initiativ, vilket inte stämde. Initiativet gick ut på att centralisera styrningen av internet till FN-organet Internationella teleunionen (ITU).[25] Även Kina har försökt att bryta den västliga dominansen genom att, bland annat, lansera egna internetprotokoll inom ITU.[26]

För det andra pågår ett arbete inom Brics för att kartlägga gemensamma möjligheter att stärka cybersäkerheten. Exakt vad som ska ingå är dock svårare att enas kring. Främst tenderar frågor om så kallad informationssäkerhet att drivas av Ryssland inom anti-extremism och anti-terrorismsamarbetet inom Brics och då hamnar fokus snabbt på trafikinnehåll snarare än funktionalitet.[27]

Det finns ett tredje område där inte minst Kina kan få stort inflytande, vilket handlar om att bygga ut internet och annan it-infrastruktur i det globala syd, där Brics kan fungera som en katalysator.[28] Kinesiska alternativ är ofta billigare än västliga konkurrenters och i vissa fall kan också Kinas infrastrukturlösningar föredras av politiska skäl, men även vara de enda som är tillgängliga – som i Rysslands fall vad gäller utbyggnaden av femte generationens mobiltelefoni.[29]

Det finns även exempel på Brics-samarbeten som stött på problem. Till följd av Edward Snowdens avslöjanden om hur amerikansk underrättelsetjänst kunnat övervaka internettrafik, lanserade Brics i början på 10-talet ett projekt som syftade till att bygga en kabel som skulle undvika USA:s infrastruktur, den så kallade Brics-kabeln (se Figur 4). Främst Sydafrika och Brasilien drev detta projekt, som ett par år senare tycks ha gått i stå på grund av bristande investeringsvilja bland Brics-länderna.[30] Under sitt ordförandeskap 2025 tog Brasilien initiativet till att försöka återstarta processen genom att lansera en teknisk och ekonomisk förstudie. Syftet beskrevs som att minska beroendet av internetinfrastruktur som kontrolleras av väst och fördjupa samarbetet inom globala syd.[31]

Generellt finns en betydande skillnad i synen på informationssäkerhet mellan å ena sidan Kina och Ryssland och å den andra Brasilien, Indien och Sydafrika. Kina och Ryssland är auktoritära länder som samarbetar

21 Stefan A. Schirm, ”Alternative World Orders? Russia’s Ukraine War and the Domestic Politics of the BRICS”, *The International Spectator*, vol. 58, nr. 3 (2023): 55–73, 61.

22 Gregory C. Allen, ”China Is Striking Back in the Tech War With the U.S”, *TIME*, 20 juli 2023; Alexander Gabuev och Oliver Stuenkel, ”The Battle for the BRICS”, *Foreign Affairs*, 24 september 2024; Caitlin Lee, ”Winning the Cold Tech War”, Rand, Santa Monica, 17 augusti 2023; Adam Segal, ”The Coming Tech Cold War With China Beijing Is Already Countering Washington’s Policy”, *Foreign Affairs*, 9 september 2020.

23 Justin Sherman, ”China’s War for Control of Global Internet Governance”, SSRN, 27 juli 2022, 15–16.

24 Maggie Miller, ”White House Agonizes over UN Cybercrime Treaty”, *Politico*, 27 september 2024; Suzanne Smalley, ”UN Cybercrime Treaty Passes in Unanimous Vote”, *The Record: Recorded Future News*, 9 augusti 2024.

25 Sherman, ”China’s War”, 15–16.

26 Edoardo Campanella och John Haigh, ”China Wants to Run Your Internet: The World’s Decentralized Internet is Coming under Competition”, *Foreign Policy*, 25 augusti 2023.

27 Ignatov, ”The BRICS Agenda”.

28 Tin Hinane El-Kadi, ”Learning along the Digital Silk Road? Technology Transfer, Power, and Chinese ICT Corporations in North Africa”, *The Information Society*, vol. 40, nr. 2 (2024): 136–53.

29 Justin Sherman, ”Huawei’s Push in Russia Exploits Kremlin Fears of Western Technology”, Atlantic Council, 18 november 2020; Maria Kolomychenko, ”The Impact and Limits of Sanctions on Russia’s Telecoms Industry”, DGAP Analysis, 2024.

30 Stacia Lee, ”International Reactions to U.S. Cybersecurity Policy”, The Heny M. Jackson School of International Studies, University of Washington, 8 januari 2016.

31 ”Brazil Reignites BRICS Submarine Cable Project with 2025 Feasibility Study Proposal”, Subsea Cables (by Telecom Review), 9 juli 2025.

**Figur 2.4** Brics-kabelns planerade sträckning.
**Källa:** Offshore Energy, ”BRICS Unveils New Submarine Cable System”, *https://www.offshore-energy.biz/brics-unveils-new-submarine-cable-system/*.

för att kontrollera sin befolkning, inte minst på det digitala området. De andra Brics-länderna har andra huvudprioriteringar. Här blir det således viktigt att djupare undersöka hur samarbetet inom Brics på cyberområdet kan utvecklas och vilka konsekvenser det skulle kunna leda till givet medlemsländernas olika prioriteringar.

### Brics framtid

Sammantaget står Brics inför en rad vägval. Att flera länder, som Colombia, Nigeria och Turkiet, har uttryckt sitt intresse för att gå med i Brics kan bli en framtida styrka.[32] Att som nu styra Brics genom konsensus utan central byråkrati kan onekligen vara en fördel, men med fler medlemmar kan den modellen bli ohållbar. Inte minst kan samarbetet prövas av Kinas inflytande och ländernas många meningsskiljaktigheter om grundläggande mänskliga fri- och rättigheter samt bilaterala spänningar mellan länder.

En kombination av redan lanserade och framtida initiativ rörande internet och annan it-infrastruktur skulle teoretiskt sett kunna lägga grunden för ett ”Bricsinternet”. Baserat på dagens medlemsländer skulle det omfatta relativt få länder men närmare hälften av jordens befolkning. Ett Brics-internet modellerat dels efter samarbetets ledande aktör på it-arenan, Kina, dels efter dess främsta förespråkare, Ryssland, skulle även sannolikt vara mer centralstyrt än dagens globala internet. Det skulle också kunna innebära att det omfattar en kärna av ytterligare frivilliga länder, inte minst Bricspartnerländer,[33] med varierande grad av regelefterlevnad bland dessa.

Bricstoppmöten följs som regel av allmänna uttalanden om samarbete och betydande framsteg, även på det digitala området. Dock tyder det faktum att samma uttalanden ofta återkommer år efter år på att praktiska åtgärder dröjer. Ett antal centrala frågor behöver således ställas i relation till ett potentiellt framtida Bricsinternet: Vad skulle ett Bricsinternet innebära rent tekniskt? Är ett Bricsinternet alls möjligt? Vilka funktioner skulle påverkas? Och om internet är ett nätverk av nätverk, vad händer om regionala kluster av nätverk inte längre ingår i samma internet och dessutom skiljs åt ideologiskt?[34] Politiska beslut om delar av det internet som växt fram till att omfatta världens alla länder under decennier kan få såväl avsedda som mindre välkomna konsekvenser.

## 2.2 Vad är internet?

Termen ”internet” omnämndes redan i kommunikationssammanhang under 1940-talet.[35] Den beskrev kommunikation från ett radionät till ett annat, ”internetwork communication”.[36] Termen kom senare att användas av systemadministratörer som kopplade

32 Patrick ”BRICS Expansion”.
33 Brics partnerländer: Belarus, Bolivia, Kuba, Kazakstan, Malaysia, Nigeria, Thailand, Uganda, Uzbekistan.
34 Mary Manjikian och Scott N. Romaniuk, ”Cybersecurity strategy and policy in a comparative context”, i *Routledge Companion to Global Cyber-Security Strategy*, red. Scott N. Romaniuk och Mary Manjikian (Abingdon och New York: Routledge, 2021): 1–7, 5.
35 ”FM 24-6 Radio Operator’s Manual, Army Ground Forces”, 1945, Internet Archive.
36 Ett radionät i denna kontext är en administrativ konstruktion där en viss grupp, till exempel en pluton, tilldelas vissa radiofrekvenser för sin användning. Normalt kommunicerar ett näts medlemmar bara med varandra men de kan ändra frekvenser och kommunicera med andra nät om det behövs.

samman datorer för att beskriva ett datornätverk som kopplade samman två eller fler lokala datornätverk. Numera används termen nästan enbart för det globala datakommunikationsnätverk som omfattar 5,5 miljarder användare eller 67,5 procent av världens befolkning. Geografiskt stora nätverk som kopplar samman en grupp mindre nät benämns numera Wide Area Network.[37]

## Paketförmedlande nätverk och dirigering

Vägen till dagens internet började med en enkel frågeställning: Hur skulle datorresurser mellan olika geografiska platser delas på ett mer effektivt sätt? I slutet av 1960-talet uppstod idén att koppla samman lokala datornät vid olika amerikanska forskningscentrum med ett gemensamt nätverk med en enda överföringsstandard för att kunna dela på datorresurser. Detta ledde till föregångaren till dagens internet, Advanced Research Projects Agency Network (Arpanet). Arpanet byggdes med utgångspunkten att maximera resursutnyttjandet av den fysiska hårdvara som utgjordes av ett antal kraftfulla datorer, belägna på olika platser i landet. För att detta skulle fungera krävdes det att forskare kunde sända meddelanden från en dator till en annan utan att koordinera med varandra, varför beslut togs om att bygga ett så kallat paketförmedlande nätverk.[38]

Det gamla analoga telenätet var ett kretskopplat nätverk. Det fungerade genom att sändaren begärde en koppling till mottagaren genom att slå ett telefonnummer, och en förbindelsekrets kopplades upp genom nätverket. Denna krets var öppen och reserverad för sändarens och mottagarens trafik under samtalets hela längd, även om ingen sade något. Detta var ineffektivt, och dessutom behövdes hela förfarandet med att koppla upp ett samtal upprepas om förbindelsen bröts.

I stället fungerar det paketförmedlande systemet så att den sändande datorn delar upp det utgående meddelandet i så kallade paket. Dessa skickas oberoende av varandra och sätts samman av den mottagande datorn vid framkomsten. Enklast är att tänka på varje paket som en blankett med olika fält som avsändare, mottagare, paketnummer och andra uppgifter som behövs för att den dator som tar emot ett paket ska kunna utläsa allt den behöver veta för att sända paketet vidare till dess destination (samt en liten del av själva meddelandet).

Detta möjliggör att många meddelanden kan sändas via en delad förbindelse utan att de olika sändarna och mottagarna behöver vänta på att andra ska lägga på. Vid ett avbrott eller störning av trafiken behöver inte hela meddelandet sändas om, utan bara de paket som gått förlorade.

Ytterligare en fördel med paketförmedlade nätverk är att paketen inte behöver ta samma väg. Om en delförbindelse är hårt belastad kan paketen sändas en annan rutt eller fördelas på flera rutter, vilket medger större trafikmängd totalt. Om paketen kommer fram i olika ordning sparar mottagardatorn dem och sätter ihop meddelandet i efterhand. Denna dirigering (*routing*) görs vid varje nytt nätsegment av maskiner som kallas ”omdirigerare” eller ”router”.

Mycket förenklat kan det sägas att dirigering fungerar så att en router håller reda på åt vilket håll i nätverket mottagaren befinner sig och hur många routrar paketen passerar på vägen dit. En router skickar sedan paketen till den första routern på den rutt som har minst antal hopp mellan routrar. Den routern upprepar i sin tur förfarandet, och så vidare.

## Internets dirigeringsnivåer

Internetleverantörer (Internet Service Providers, ISP:er) brukar delas in i tre nivåer. Nivå 3-leverantörer är de leverantörer som tillhandahåller internetuppkoppling till slutanvändare, vilket kan vara privatpersoner, företag eller organisationer. Dessa leverantörer ansvarar för att skicka och ta emot data till och från användarnas enheter, exempelvis via fibermodem eller mobilnät. Eftersom nivå 3-leverantörer saknar ett eget globalt nätverk måste de köpa kapacitet från nivå 2-leverantörer för att kunna skicka trafik utanför sitt eget nät.

Nivå 2-leverantörer driver större nätverk som kopplar samman flera nivå 3-leverantörer. De fungerar som mellanhänder som transporterar trafik mellan lokala internetleverantörer och det globala internet. En nivå 2-leverantör kan ha egna kunder, men deras huvudsakliga roll är att vidareförmedla trafik åt nivå 3-leverantörer. För att få global räckvidd betalar nivå 2-leverantörer nivå 1-operatörer för att transportera trafik mellan olika regioner och länder.

Nivå 1-operatörer är de största aktörerna i internetinfrastrukturen och driver de primära globala datanäten. De har kapacitet att transportera trafik mellan kontinenter och har direktanslutningar till andra nivå 1-leverantörer. Till skillnad från nivå 2 och 3 betalar nivå 1-operatörer inte någon annan för att skicka trafik. Istället utbyter de trafik med andra nivå 1-operatörer

37 Statista, ”Number of internet and social media users worldwide as of February 2025 (in billions)”, 13 februari 2025.

38 Lawrence G. Roberts, ”Multiple Computer Networks and Intercomputer Communication”, *SOSP ‘67: Proceedings of the first ACM symposium on Operating System Principles* (1967): 3.1–3.6.

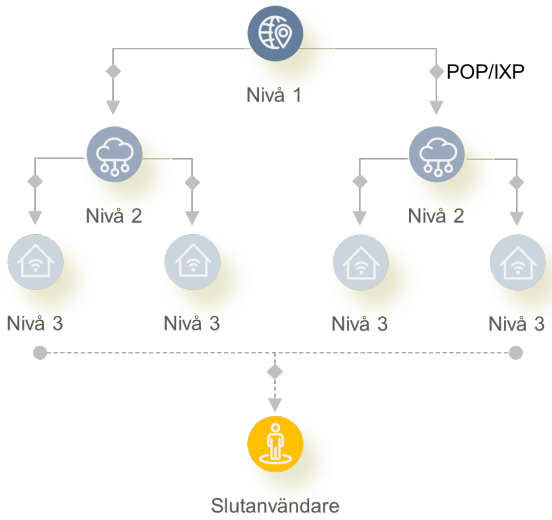
genom så kallad *peering*, vilket gör att de kan hantera globala dataflöden utan externa avgifter (se Figur 2.5).[39]

Mellan varje ISP finns det en eller flera fysiska knutpunkter, i praktiken stora datorhallar. Dessa platser kallas *point of presence* (POP) eller *Internet Exchange Points* (IXP:er). Detta är platser där olika nät fysiskt sammanstrålar och informationspaketen kan flyttas mellan olika operatörers nät. Två specialfall av dessa är satellitstationer och undervattenskablar. Från en satellitstation sänds data i radioform till kommunikationssatelliter och i en undervattenskabel sänds data i elektronisk eller optisk form långa sträckor under hav. I teorin flödar internettrafiken genom nätverken helt beroende på belastning och tillgängliga routrar, men i praktiken ser det annorlunda ut, bland annat beroende på bandbredd.

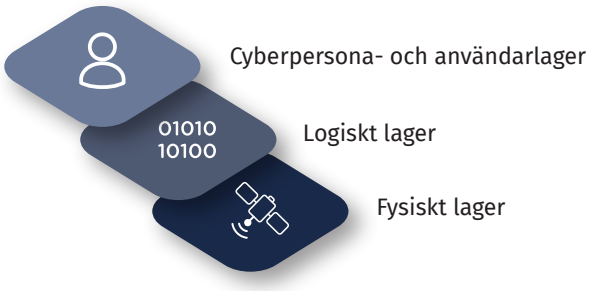
Utbyggnaden av den fysiska infrastrukturen följer till stor del samma mönster som det gamla analoga telenätet. I ett hus eller fabrik finns en lokal växel, en nivå 3-leverantör. I en stad finns ett lokalt bolag som skickar sin trafik mellan sina abonnenter och till en nivå 2-leverantör på riksnivå, och överst finns nivå 1-leverantörer vilka utgörs av internationella och interkontinentala företag med satellitlänkar och kablar. Det här upplägget innebär att internationell trafik från Sverige i princip alltid passerar vad som ursprungligen var TeliaSoneras nätverk Telia Carrier (idag en del av Arelion) eftersom Telia var det företag som ursprungligen byggde upp grunden i den svenska internetinfrastrukturen.

## Internet och cyberdomänens lager

Internet består inte endast av teknisk infrastruktur och digital kommunikation. Mjukvara och mänskliga användare av internet är minst lika viktiga. I rapporten används prefixet ”cyber” som en övergripande term för att beskriva områden relaterade till digitala data, digital kommunikation, internet och it-infrastruktur. I detta sammanhang omfattar ”cyberdomänen” både




**Figur 2.5** Internets dirigeringsnivåer.




**Figur 2.6** Cyberdomänens lager. Modell hämtad från Försvarsmakten, ”Doktrininsats: Cyberförsvar”, DA CYBER 2024, Versionsnr. 1.1.

39 Beskrivningen är förenklad. China Telecom brukar till exempel klassas som en ”regional nivå 1-leverantör” eftersom bolaget inom Kina fungerar som en nivå 1, men globalt måste betala för att reläa trafik.

de tekniska system som möjliggör digital information och de tekniker som används för att hantera, lagra och överföra denna information, samt människorna som använder sig av detta.

För att konceptualisera cyberdomänen används en inom försvarskretsar etablerad modell som delar upp domänen i tre lager (se figur 2.6). Det fysiska lagret är det som ofta refereras till som ”hårdvara”, t.ex. datorer, servrar och kablar. Det logiska lagret består av t.ex. programkod och protokoll och behöver ett fysiskt lager för att existera. Cyberpersona- eller användarlagret är användares virtuella identiteter (t.ex. en mejladress, eller ett id på sociala medier). En användare kan ha många virtuella identiteter, vilket i sin tur bygger på det logiska lagret.

Som tidigare har beskrivits lägger den här rapporten huvudfokus på de fysiska och logiska lagrens betydelse för utvecklingen av ett potentiellt Brics-internet. Det innebär de olika författarna till landkapitlen beskriver de val som respektive land har gjort, och eventuellt planerar att göra i dessa lager.

## Reglering av internet

Under Arpanet:s tid var det enbart ickekommersiella organisationer som fick använda nätverket. 1975 fick den första kommersiella datanätverksleverantören tillstånd att starta sin verksamhet med Telenet, en datakommunikationsservice med dataväxlar i sju städer från Kalifornien till New York. Till dessa ringde kunderna med telefonmodem via det vanliga telenätet. Men Telenet hade inga kopplingar till Arpanet, eller resten av världen.

Under de följande åren togs ett antal olika initiativ i olika länder för att koppla samman olika statliga, vetenskapliga och akademiska organisationer. Men inte förrän 1988 tilläts kommersiella tillämpningar att kopplas samman med de statliga satsningarna. Det amerikanska National Science Foundation Network (Nfsnet) fick då tillstånd att på experimentell basis reläa mejltrafik från ett antal kommersiella datakommunikationsföretag; utöver Telenet tillkom MCI Mail, Tymnet och Compuserve. Dessa företag kunde nu inte bara nå sina egna kunder via Nfsnet, utan även varandras kunder.

På kort tid startades fler företag för att möta efterfrågan på datakommunikation. Nya kopplingar skedde till Nfsnet, men också mellan de olika anslutna organisationerna. Företagen upptäckte att de tjänade mer på att reläa varandras trafik (för pengar, eller att få sin egen trafik reläad) än att försöka låsa in sina kunder.

Detta ledde fram till dagens internet där omkring 120 000 företag och organisationer, samarbetar med att sända varandras trafik över hela världen.[40] En viktig aspekt av i denna utveckling har varit att sätta tekniska standarder för internets arkitektur och digitala innehåll. Internationella standarder rör dock inte endast teknik och kommunikation utan handlar även om överenskomna regler och riktlinjer för att säkerställa processers, tjänsters och produkters säkerhet och kompatibilitet,[41] vilket underlättar internationell handel och kommunikation.[42]

Idag finns relativt välkända standarder, exempelvis för trådlöst internet (Wi-Fi, IEEE 802.11), tilldelning av IP-adresser (IPv4 och IPv6), överföring av data och elektricitet mellan datorer och olika enheter (USB), webbsidors uppbyggnad och funktion (HTML, CSS och http/HTTPS) och TCP/IP (Transmission Control Protocol och Internet Protocol), vilket är internets grundläggande standard för kommunikation över internet.

Standarder utvecklas av standardutvecklande organisationer (SDO) där den största internationella organisationen är Internationella standardiseringsorganisationen (ISO). När det gäller standardisering av internet och it-infrastruktur finns ingen enskild övergripande organisation. De mest centrala är: Internets tekniska ledningsgrupp (IETF); Internet Corporation for Assigned Names and Numbers (ICANN); World Wide Web Consortium (W3C); det amerikanska Institute for Electrical and Electronics Engineers (IEEE); det europeiska European Telecommunications Standards Institute (ETSI); och Internationella teleunion (ITU). Alla dessa organisationer består i princip icke-statliga organisationer och industrin, utom ITU som är ett FN-organ. Eftersom internets standardiseringsprocesser är så pass heterogena och decentraliserade är det svårt för en enskild stat att kontrollera dem. Det finns dock starka ekonomiska incitament att sätta standarder för företag eftersom standardisering av patenterad teknik innebär royalties och ett försprång på marknaden.[43] Från

40 ”Regional Internet Registries Statistics”, 1 september 2025.

41 Exempel på standarder är: ISO 14001 (riktlinjer för miljöledning, exempelvis hur företag kan minska sin miljöpåverkan); IEC 60335 (säkerhet för elektriska hushållsapparater som mikrovågsugnar och kylskåp); ITU H.264 (teknik för videokodning som bland annat används i VTC-program och av YouTube).

42 Craig N. Murphy and JoAnne Yates, *The International Organization for Standardization (ISO): Global Governance through Voluntary Consensus* (London och New York: Routledge, 2009), 46–47.

43 Matt Sheehan och Jacob Feldgoise, ”What Washington Gets Wrong About China and Technical Standards”, *Carnegie Endowment for International Peace*, 27 februari 2023.

ett statligt perspektiv kan det handla om att främja sina egna företags tekniska lösningar samt normer och värderingar på den internationella arenan.[44]

Historiskt sett har amerikanska och europeiska aktörer varit ledande i standardisering av internet och it-infrastruktur genom flerpartsstyrning. Den amerikanska och den europeiska modellen för standardisering skiljer sig dock åt något där den tidigare helt och hållet är privat medan den europeiska består av privat-statligt samarbete.[45] De tidigare nämnda ryska och kinesiska initiativen handlar om att bryta flerpartsstyrningen för en mellanstatlig modell där ländernas makt över standarder och det globala internet potentiellt sätt skulle kunna stärkas, exempelvis genom stöd från Brics medlems- och partnerländer.

## 2.3 Säkerhetskonsekvenser av internets infrastruktur

Information har alltid varit av intresse för nationer, företag och andra organisationer. Generellt sett har exempelvis stater samlat information inom rad olika områden genom öppna kanaler, via underrättelser och spionage riktat mot såväl egna medborgare som länder och deras medborgare och ickestatliga organisationer. Information är även en viktig handelsvara på den kriminella arenan.

Eftersom internet idag är den väg genom vilken en majoritet av all världens information sänds är naturligtvis internet ett av de största målen för alla dessa ändamål. Medan detta gäller för internets alla lager fokuserar vi här på det fysiska lagret. För informationsinhämtning är intressepunkter där stora mängder data passerar, nämligen undervattenskablar, IXP:er och POP:ar. Om det går att placera personal eller avlyssningsutrustning på dessa platser kan informationsvinsten bli mycket stor.

### Dirigering

I och med att dirigering av datapaket är en form av rutt-system där data går genom olika typer av routrar är de senare en intressepunkt för informationsinsamling. Den som kontrollerar routern kan se vilka datorer som skickar meddelanden via den, och därmed kartlägga trafikmönster. Om meddelandets innehåll inte krypterats kan den som kontrollerar routern kopiera paket och extrahera meddelandebitar från dem. Den som kontrollerar routern kan även blockera viss trafik, eller göra den långsammare genom att sända paket på avvägar eller kasta dem.

Därför är kontrollen över strategiskt placerade routrar av högt värde för underrättelsetjänster och industrispioner som kan få viktig information men också för exempelvis stater som skulle vilja isolera delar av internet från varandra eller blockera viss trafik inom sitt territorium.

### Kabelavlyssning

Innan internets tillkomst användes markbundna och undervattenskablar för telekommunikation och det finns flera kända historiska exempel på avlyssning. Amerikansk underrättelsetjänst lyckades exempelvis att placera avlyssningsutrustning på en stor televäxel i Östberlin och en central sovjetisk undervattenskabel under kalla kriget.[46] Det är naturligtvis inte enbart USA som avlyssnar internet. Storbritanniens signalunderrättelseorganisation har avlyssningsstationer både inom och utom landet,[47] och auktoritära regeringar har länge försökt att avlyssna kommunikation både mellan egna medborgare och mellan det egna landet och omvärlden.[48] Genom att avlyssna internettrafik via kablar kan trafikens säkerhetsskydd (som mindre avancerad kryptering) kringgås. De flesta länder har dock inte den kapacitet som behövs för att avlyssna djuphavskablar, men alla kablar kommer i land någonstans. Om en aktör kan ta kontroll över de datacenter som kablarna ansluter till har de i praktiken möjlighet att avlyssna trafiken.

Som framgår i Figur 7 ligger USA väl till när de gäller att avlyssna kabeltrafik när den når land. En stor del av internettrafiken mellan Europa, Sydamerika och Asien passerar USA. Dessutom har USA underrättelsesamarbeten med länder i Afrika och Mellanöstern, som Egypten, Djibouti, Oman m.fl., och kan möjligtvis få

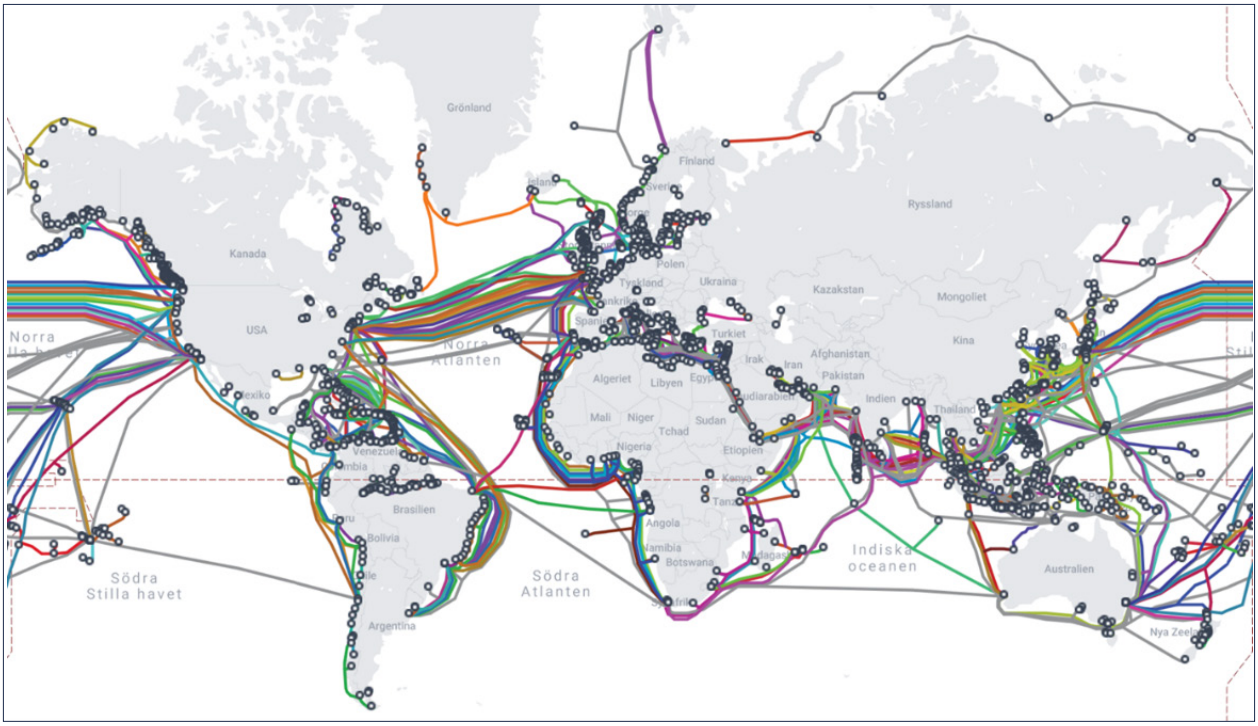
44 Edoardo Campanella och John Haigh, ”The Battle for the Internet”, *Survival*, vol. 66, nr. 1 (2024): 69–84, 73.

45 Tim Rühlig, *Technical Standardisation, China and the Future International Order* (Bryssel: Heinrich Böll Stiftung, 2020), 12.

46 Se: CIA, ”Clandestine Services history The Berlin Tunnel Operation 1952-1956”, CS Historical paper, nr. 150, 1968; Europaparlamentet, ”Development of surveillance technology and risk of abuse of economic information – Appraisal of Technologies of Political Control”, vol. 2/5, EU/STOA 1999.

47 Duncan Campbell, ”Revealed: GCHQ’s beyond top secret Middle Eastern internet spy base Snowden leaks that UK.gov suppressed”, *The Register*, 3 juni 2014.

48 Se: Ron Deibert, ”Cyberspace under Siege”, *Journal of Democracy*, vol. 26, nr. 3, 2015, 64–78.




**Figur 2.7** Undervattenskabelkarta, Submarine Cable Map (Creative Commons License: CC BY-SA 4.0).[(a)]

**Anm: (a)**Telegeography, "Submarine Cable Map", 1 september 2025. De runda prickarna representerar landfästen (landing points), d.v.s. den fysiska plats där sjökablar ansluter

tillgång till kablarna när de passerar dessa länders IXP:er och POP:ar.[49]

## Serviceavbrott

Det är också värdefullt att kunna beröva motståndaren information. Även här har knutpunkterna för ledningar och kablar varit föremål för angrepp sedan deras införande. Till exempel var den första operationen Storbritannien utförde efter att de deklarerat krig mot Tyskland 1914 att skicka ett kabelläggarskepp, *Alert*, för att kapa Tysklands telegrafkablar över Atlanten.[50] Idag är sabotage mot undervattenskablar ett alternativ för att försämra ett lands kommunikationsmöjligheter, men med risken att ett kabelbrott inte stoppar trafiken för enbart ett land utan för många.

Trafik kan sorteras utifrån ursprung, destination, och många andra faktorer eftersom detta är en normal del av den dirigering som internet utför. Så den som kontrollerar växlarna kan programmera om dem att behandla viss trafik annorlunda. Detta möjliggör för de länder som kontrollerar IXP:er och POP:ar, i synnerhet sådana där stora kablar ansluter, att strypa förbindelser, eller sortera bort viss trafik om de så skulle vilja. Detta kan användas som en del i ekonomisk krigföring, sanktioner, eller för andra syften, och då kommer paketbaserad kommunikation in i bilden igen. Om vissa vägar är blockerade kan det, beroende på situationen, vara möjligt att kringgå blockaden genom att använda alternativa vägar. Det beror dock på en rad faktorer, om sådana vägar finns och om de kan hantera trafikökningen.

## Hårdvara, produktion och leverantörskedjor

Dagens globala leverantörskedjor och produktionen av hårdvara för internets fysiska lager utgör ännu en kritisk risk. Komponenter kommer ofta från flera länder och underleverantörer som var och en hanterar sina egna delprocesser, från brytning av sällsynta jordartsmetaller till montering av kompletta moderkort. Brist på *transparens* och *spårbarhet* innebär att en användare av hårdvaran sällan vet exakt var en viss komponent har

49 Michele Black och Osamah Alhenaki, "Business as Usual: The Egyptian–U.S. Intelligence Relationship", *Global Security and Intelligence Studies,* vol. 1, nr. 1 (2015): 14–30; United States Department of State, "U.S. Security Cooperation with Oman"; David Vergun, "DOD Supports African Partner Nations in Multiple Ways", U.S. Department of Defense, 1 maj 2020.

50 Rhodri Jeffreys-Jones, *In Spies We Trust: The Story of Western Intelligence*, (Oxford University Press, 2013), 43.

producerats eller vilka aktörer som har varit inblandade.[51] Vidare är produktion av kritiska komponenter koncentrerat till ett fåtal aktörer som skapar beroendeställningar som kan utnyttjas för säkerhetspolitiska vinningar.[52]

Antagonistiska aktörer kan vidare manipulera hårdvara under tillverkning, transport eller lagerhållning och införa dolda mikroprocessorer, bakdörrar i fast programvara (*firmware*) eller modifierade kretskort. Manipulerad hårdvara är svår att upptäcka och kan ge permanent åtkomst till de system som de installeras i.[53]

## 2.4 Sammanfattning

Detta här kapitlet har övergripande beskrivit Brics utveckling som en geopolitisk aktör med fokus på cyberområdet, där spänningen mellan splittring och enighet är central. Samarbetet har vuxit i omfång och betydelse där Kina framstår som den tekniska och teknologiska stormakten, både inom Brics och globalt. På cyberområdet betonas strävan efter ökad autonomi från väst och ett större inflytande över de institutioner och regler som styr internet. Samtidigt synliggörs en intern skiljelinje inom Brics, där framför allt Kina och Ryssland förespråkar starkare statlig kontroll över innehåll och informationsflöden.

Kapitlet har även placerat internets utveckling i ett analytiskt ramverk genom att beskriva internet i tre lager: cyberpersona- och användarlagret, det logiska lagret och det fysiska lagret. I rapporten läggs särskilt fokus på det fysiska lagret och i viss mån det logiska lagret samt på säkerhetspolitiska aspekter som rör frågor om infrastruktur, ägandeförhållanden, leverantörskedjor och strategiska beroenden i en global ekonomi.

Avslutningsvis har kapitlet identifierat ett antal nyckelfrågor som leder vidare till rapportens fortsatta analys: Vad skulle ett ”Bricsinternet” innebära i teknisk mening, och är det ens genomförbart? Hur försöker länderna öka sin kontroll över kritiska funktioner för att öka sin cybersäkerhet? Vilka funktioner i det globala nätverket skulle påverkas av en ökad uppdelning av internet i ett västligt och ett ”Bricsinternet”? Och vad händer med internet som idé om regionala kluster av nät skiljs åt, både tekniskt och ideologiskt? Dessa frågor undersöks vidare i de följande kapitlen genom fördjupade landanalyser, där Brics-medlemmarnas respektive strategier, ambitioner och handlingsutrymme analyseras i detalj.

51 Christian Goodwin och Joram Borenstein, ”Guarding against supply chain attacks—part 2: Hardware risks”, Microsoft: Compliance, 3 februari 2020.

52 Henry Farrell och Abraham L. Newman, ”Weaponized Interdependence: How Global Economic Networks Shape State Coercion”, *International Security,* vol. 44, nr. 1: 42–79; Henry Farrell och Abraham L. Newman, ”The Weaponized World Economy: Surviving the New Age of Economic Coercion”, *Foreign Affairs*, 19 augusti 2025.

53 Mohammad Monjur, Joshua Calzadillas och Qiaoyan Yu, ”Hardware Security Risks and Tthreat Analysis in Advanced Manufacturing Industry”, *ACM Transactions on Design Automation of Electronic Systems*, vol. 28, nr. 5 (2023): artikel nr. 83, 1–22.

# Referenser

”Brazil Reignites BRICS Submarine Cable Project with 2025 Feasibility Study Proposal”, Subsea Cables (by Telecom Review). 9 juli 2025, hämtad 4 februari 2026, *https://www.subseacables.net/industry-news/brazil-reignites-brics-submarine-cable-project-with-2025-feasibility-study-proposal/*.

”FM 24-6 Radio Operator’s Manual, Army Ground Forces”, 1945, Internet Archive, hämtad 1 september 2025, *https://archive.org/details/Fm24-6/mode/2up?q=internet*.

”Global North and Global South”, Britannica. 29 augusti 2025, *https://www.britannica.com/topic/Global-North-and-Global-South*.

”Regional Internet Registries Statistics”. 1 september 2025, *https://www-public.telecom-sudparis.eu/~maigron/rir-stats/rir-delegations/world/world-asn-by-number.html*.

Allen, Gregory C. ”China Is Striking Back in the Tech War With the U.S”. *TIME*, 20 juli 2023.

Black, Michele och Osamah Alhenaki. ”Business as Usual: The Egyptian–U.S. Intelligence Relationship”. *Global Security and Intelligence Studies*, vol. 1, nr 1 (2015): 14–30.

Campanella, Edoardo och John Haigh. ”China Wants to Run Your Internet: The World’s Decentralized Internet is Coming under Competition”. *Foreign Policy*. 25 augusti 2023, hämtad 4 november 2024, *https://foreignpolicy.com/2023/08/25/china-wants-to-run-your-internet/*.

Campanella, Edoardo och John Haigh. ”The Battle for the Internet”. *Survival*, vol. 66, nr. 1 (2024): 69–84.

Campbell, Duncan. ”Revealed: GCHQ’s beyond top secret Middle Eastern internet spy base Snowden leaks that UK.gov suppressed”. *The Register*. 3 juni 2014, hämtad 2 februari 2024, *https://www.theregister.com/2014/06/03/revealed_beyond_top_secret_british_intelligence_middleeast_internet_spy_base/*.

CIA. ”Clandestine Services history The Berlin Tunnel Operation 1952–1956”, CS Historical Paper No. 150, 1968, hämtad 1 september 2025, *https://www.cia.gov/readingroom/docs/CIA-RDP07X00001R000100010001-9.pdf*.

Deibert, Ron. ”Cyberspace under Siege”, *Journal of Democracy*, vol. 26, nr. 3 (2015): 64–78.

Duggan, Niall och Juan Carlos Ladines Azalia. ”From Yekaterinburg to Brasilia: BRICS and the G20, Road to Nowhere?” *Revista Brasileira de Política Internacional*, vol. 63, nr. 1 (2020): e009.

Duggan, Niall Bas Hooijmaaijers, Marek Rewizorski och Ekaterina Arapova. ”Introduction: ’The BRICS, Global Governance, and Challenges for South–South Cooperation in a Post-Western World’”. *International Political Science Review*, vol. 43, nr. 4 (2022): 469–80.

Europaparlamentet. ”Development of surveillance technology and risk of abuse of economic information – Appraisal of Technologies of Political Control”, vol. 2/5, EU/STOA 1999, hämtad 1 september 2025, *https://www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET(1999)168184_EN.pdf*.

Farrell, Henry och Abraham L. Newman. ”Weaponized Interdependence: How Global Economic Networks Shape State Coercion”. *International Security*, vol. 44, nr. 1: 42–79.

Farrell, Henry och Abraham L. Newman. ”The Weaponized World Economy: Surviving the New Age of Economic Coercion”. *Foreign Affairs*. 19 augusti 2025, hämtad 1 september 2025, *https://www.foreignaffairs.com/united-states/weaponized-world-economy-farrell-newman*.

Försvarsmakten. ”Doktrinansats Cyberförsvar”. DA CYBER 2024, Versionsnr. 1.1., hämtad 1 september, 2024, *https://www.forsvarsmakten.se/contentassets/e61862b2384e42878adcb5cc303b5362/doktrinansats-cyberforsvar-1.1-bilaga-1.pdf*.

Gabuev, Alexander och Oliver Stuenkel. ”The Battle for the BRICS: Why the Future of the Bloc Will Shape Global Order”. *Foreign Affairs*. 24 september 2024, *https://www.foreignaffairs.com/russia/battle-brics*.

Goodwin, Christian och Joram Borenstein. ”Guarding against supply chain attacks—part 2: Hardware risks”. Microsoft: Compliance. 3 februari 2020, hämtad 1 september 2025, https://www.microsoft.com/en-us/security/blog/2020/02/03/guarding-against-supply-chain-attacks-part-2-hardware-risks/.

Hinane El-Kadi, Tin. ”Learning along the Digital Silk Road? Technology Transfer, Power, and Chinese ICT Corporations in North Africa”. *The Information Society*, vol. 40, nr. 2 (2024): 136–53.

Hooijmaaijers, Bas. ”China, the BRICS, and the Limitations of Reshaping Global Economic Governance”. *The Pacific Review*, vol. 34, nr. 1 (2021): 29–55.

Hooijmaaijers, Bas och Stephan Keukeleire. ”Voting Cohesion of the BRICS Countries in the UN General Assembly, 2006−2014: A BRICS Too Far?” *Global Governance: A Review of Multilateralism and International Organizations*, vol. 22, nr. 3 (2016): 389–408.

Ignatov, Aleksandr. ”The BRICS Agenda on the Internet Governance”. *International Organisations Research Journal*, vol. 17, nr. 2 (2022): 86–109.

Jeffreys-Jones, Rhodri. *In Spies We Trust: The Story of Western Intelligence*. Oxford University Press, 2013.

Jiang, Tianjiao. ”The Shift of China’s Strategic Thinking on Cyberwarfare Since the 1990s”, *Journal of Chinese Political Science*, vol. 28, nr. 1 (2023): 127–49.

Kolomychenko, Maria. ”The Impact and Limits of Sanctions on Russia’s Telecoms Industry”. *DGAP Analysis*, German Council of Foreign Relations, 2024. hämtad 7 november 2024, *https://dgap.org/system/files/article_pdfs/DGAP_Analysis_No-3_March%202026.pdf*.

Kreml. ”Obrasjtjenije Vladimira Putina v svjazi s natjalom predsedatelstva Rossii v BRIKS” [Vladimir Putins anförande i samband med inledningen av Rysslands ordförandeskap i BRICS]. 1 januari 2024, hämtad 22 juli 2024 *kremlin.ru/events/president/news/73202*.

Lee, Caitlin. ”Winning the Cold Tech War”. Rand, Santa Monica. 17 augusti 2023, hämtad 4 november 2024, *https://www.rand.org/pubs/commentary/2023/08/winning-the-tech-cold-war.html*;

Lee, Stacia. ”International Reactions to U.S. Cybersecurity Policy: the BRICS undersea cable”, The Heny M. Jackson School of International Studies, University of Washington. 8 januari 2016, hämtad 1 september 2025, *https://jsis.washington.edu/news/reactions-u-s-cybersecurity-policy-bric-undersea-cable/*.

Pesha Magid, Maha El Dahan och Manya Saini. ”Saudi Arabia sits on fence over BRICS with eye on vital ties with US”. *Reuters*. 8 maj 2025, hämtad 4 februari 2026, *https://www.reuters.com/world/middle-east/saudi-arabia-sits-fence-over-brics-with-eye-vital-ties-with-us-2025-05-08/*.

Manjikian, Mary och Scott N. Romaniuk. ”Cybersecurity strategy and policy in a comparative context”. I *Routledge Compansion to Clobal Cyber-Security Strategy*, red. Scott N. Romaniuk och Mary Manjikian. Abingdon och New York: Routledge, 2021.

Miller, Maggie. ”White House agonizes over UN cybercrime treaty”. *Politico*. 27 september 2024, hämtad 4 november 2024, *https://www.politico.com/news/2024/09/26/un-cybercrime-treaty-white-house-russia-00181271*.

*Mohammad Monjur, Joshua Calzadillas och Qiaoyan Yu. ”Hardware Security Risks and Tthreat Analysis in Advanced Manufacturing Industry”. ACM Transactions on Design Automation of Electronic Systems, vol. 28, nr. 5 (2023): artikel nr. 83: 1–22.*

Murphy, Craig N. and JoAnne Yates. *The International Organization for Standardization (ISO): Global Governance through Voluntary Consensus*. London och New York: Routledge, 2009.

O’Neill, Jim. *Building Better Global Economic BRICs*, Goldman Sachs, Global Economics Paper. nr. 66, 2001, hämtad 22 juli 2024, *https://www.goldmansachs.com/intelligence/archive/archive-pdfs/build-better-brics.pdf*.

Pant, Harsch V. ”The BRICS Fallacy”. *The Washington Quarterly*, vol. 36, nr. 3 (2013): 91–105.

Patrick, Stewart. ”BRICS Expansion, the G20, and the Future of World Order”, Carnegie Endowment for International Peace. 9 oktober 2024, hämtad 4 november 2024, *https://carnegieendowment.org/research/2024/10/brics-summit-emerging-middle-powers-g7-g20?lang=en*.

Raman, G. Venkat och Rajan Kumar. ”Introduction”. I *Locating BRICS in the Global Order*, red. Rajan Kumar, Meeta Keswani Mehra, G. Venkat Raman, och Meenakshi Sundriyal (London and New York: Routledge, 2023).

Roberts, Cynthia. ”Polity Forum: Challengers or Stakeholders? BRICs and the Liberal World Order”. *Polity*, vol. 42, nr. 1 (2010): 1–13.

Roberts, Lawrence G. ”Multiple Computer Networks and Intercomputer Communication”. *SOSP ’67: Proceedings of the first ACM symposium on Operating System Principles* (1967): 3: 1–6.

Rühlig, Tim, *Technical Standardisation, China and the Future International Order*. Bryssel: Heinrich Böll Stiftung, 2020. hämtad 1 september 2025, *https://eu.boell.org/sites/default/files/2020-03/HBS-Techn%20Stand-A4%20web-030320.pdf*.

Schirm, Stefan A. ”Alternative World Orders? Russia’s Ukraine War and the Domestic Politics of the BRICS”. *The International Spectator*, vol. 58, nr. 3 (2023): 55–73. *https://www.tandfonline.com/doi/full/10.1080/03932729.2023.2236937* (2024-07-22).

Segal, Adam. ”The Coming Tech Cold War With China Beijing Is Already Countering Washington’s Policy”. *Foreign Affairs*. 9 september 2020, hämtad 4 november 2024, *https://www.foreignaffairs.com/articles/north-america/2020-09-09/coming-tech-cold-war-china*.

Sheehan, Matt och Jacob Feldgoise. ”What Washington Gets Wrong About China and Technical Standards”. *Carnegie Endowment for International Peace*. 27 februari 2023, hämtad 1 september 2025, https://carnegieendowment.org/research/2023/02/what-washington-gets-wrong-about-china-and-technical-standards?lang=en.

Sherman, Justin. ”China’s War for Control of Global Internet Governance”. SSRN. 27 juli 2022, *https://dx.doi.org/10.2139/ssrn.4174453*.

Sherman, Justin. ”Huawei’s Push in Russia Exploits Kremlin Fears of Western Technology”. Atlantic Council. 18 november 2020, hämtad 7 november 2024, *https://www.atlanticcouncil.org/blogs/new-atlanticist/huaweis-push-in-russia-exploits-kremlin-fears-of-western-technology/*

Smalley, Suzanne. ”UN Cybercrime Treaty Passes in Unanimous Vote”. *The Record: Recorded Future News*. 9 augusti 2024, hämtad 4 november 2024, *https://therecord.media/un-cybercrime-treaty-passes-unanimous*.

Statista. ”Number of internet and social media users worldwide as of February 2025 (in billions)”, 13 februari 2025, *https://www.statista.com/statistics/617136/digital-population-worldwide/*.

Strokan, Sergej. ”Planeta BRIKS” [Bricsplaneten], *Kommersant*, 27 december 2024, hämtad 9 januari 2025, *https://www.kommersant.ru/doc/7363881*.

Stuenkel, Oliver. *The BRICS and the Future of Global Order*. Lanham, Boulder, New York och London: Lexington Books, 2020.

Telegeography, ”Submarine Cable Map”. 1 september 2025, *https://www.submarinecablemap.com/*.

United States Department of State. ”U.S. Security Cooperation with Oman”, hämtad 20 januari 2025, *https://www.state.gov/u-s-security-cooperation-with-oman/*.

Vergun, David. ”DOD Supports African Partner Nations in Multiple Ways”. U.S. Department of Defense. 1 maj 2020, hämtad 28 februari 2025, *https://www.defense.gov/News/News-Stories/Article/Article/2172908/dod-supports-african-partner-nations-in-multiple-ways/*.

Världsbanken, ”Population, total”. 2 oktober 2024, *https://data.worldbank.org/indicator/SP.POP.TOTL*.

World Economic Outlook Database. *https://www.imf.org/en/Publications/WEO/weo-database/2025/April*.

Zuma, Jacob. ”Durban Summit: Plenary Address”. BRICS Information Centre, Toronto University. 27 mars 2013, *http://www.brics.utoronto.ca/docs/130327-zuma-address.html*.

# 3. Brasilien – en balanserande regional makt

*Olivier Milland*

Brasilien är en sydamerikansk stormakt med ambitioner om att öka sin internationella status. Detta gör Brasilien bland annat genom att skaffa sig en ledarroll inom olika internationella organisationer och forum, som Brics. Dock vill Brasilien vidmakthålla diversifierade internationella relationer för att försäkra sig om att kunna föra en självständig utrikes- och säkerhetspolitik, och för att inta en strategisk position mellan olika maktpoler, som USA, Kina och Europa. Det har resulterat i en politik som kan uppfattas som tvetydig och ombytlig av externa aktörer. Samtidigt signalerar den att Brasilien med stor sannolikhet kommer att bromsa ned en fördjupning av Brics-samarbetet om det inte ligger i landets egna intressen.

## 3.1 Brasiliens relation till Brics

Brasilien uppfattar huvudsakligen Brics som ett verktyg för att uppnå högre internationell status. Sakfrågor som Brasilien har prioriterat är ekonomiska samarbeten och reformer av den globala styrningen, även om frågor som rör fred och säkerhet har fått större utrymme vid Brics-toppmöten de senaste femton åren.[1]

För Brasiliens del handlar Brics om att etablera ett forum med andra likasinnade stater som vill utmana traditionella maktstrukturer, framförallt de som domineras av väst. Dock vill Brasilien inte ersätta maktstrukturerna utan använder istället nya internationella forum som ett verktyg för att skapa sig en ledarroll och klättra inom de befintliga organisationerna. Ansatsen kallas ibland för *soft-balancing* inom internationella relationer.[2] Samarbetet mellan Brics-länderna har lett till konkreta utrikespolitiska framgångar för Brasilien. Bland annat koordinerar medlemsländerna sin positionering i sakfrågor inom San Fransisco- (framförallt FN:s säkerhetsråd och Världshandelsorganisationen) och Bretton Woods-institutionerna.[3] Inom de senare har Brasiliens andel röster utvidgats i både Internationella valutafonden och Världsbanken.[4] Brics-länderna fortsätter att samarbeta för ytterligare reformer av dessa institutioner.[5]

På samma sätt har Brasilien kunnat utnyttja Brics-samarbetet för att nå framgångar i andra forum. I utbyte för Brasiliens stöd för kinesisk- och ryskledda utvidgningsprocessen av Brics 2023 uppges president Luiz Inácio Lula da Silva (bäst känd under smeknamnet Lula) exempelvis ha krävt Kinas stöd för Brasiliens anspråk på en permanent plats i FN:s säkerhetsråd och att detta inkluderades i uttalandet från Brics-toppmötet i Sydafrika 2023.[6]

Även om säkerhetsrelaterade frågor fått högre prioritet på Brics-toppmötena så finns det få tecken på att Brasilien vill fördjupa samarbetet på detta område. Brasiliens säkerhetspolitiska mål om suveränitet och strategisk autonomi riskerar att undermineras av ett fördjupat Brics-samarbete på säkerhetsområdet. Brasilien tolkar dock, i enlighet med Brics-kommunikéerna, säkerhet som kopplad till utveckling, dvs. utan utveckling finns ingen säkerhet och vice versa.[7]

1 Leonardo Ramos, Pedro D. Rocha och Danny Zahreddine, ”A Agenda de Segurança Internacional no BRICS (2009–2019)”, *Dados,* vol. 64, nr. 3 (2021): 1–33; Zhen Han och Mihaela Papa, ”Brazilian alliance perspectives: towards a BRICS development-security alliance?”, *Third World Quarterly*, vol. 45, nr. 5 (2021), 1115–36.

2 Gelson Fonseca Jr., ”BRICS: Notes and questions” i *Brazil, BRICS and the international agenda*, red. José Vicente de Sá Pimentel, Brasília: Fundação Alexandre Gusmão, 19–45; Zhen Han och Mihaela Papa, ”Brazilian alliance perspectives: towards a BRICS development-security alliance?”

3 Maria Edileuza Fontenele Reis, ”BRICS: Genesis and evolution” i *Brazil, BRICS and the international agenda*, red. José Vicente de Sá Pimentel, Brasília: Fundação Alexandre Gusmão, 47–71; Lissandra Paragassu, ”BRICS finance ministers make unified proposal for IMF reforms”, Reuters, 5 juli 2025.

4 Mark Weisbrot och Jake Johnston, ”Voting Share Reform at the IMF: Will it Make a Difference?”, Washington, DC: Center for Economic and Policy Research, 2010; Jakob Vestergaard, ”Voice Reform in the World Bank”, 2010, Danish Institute of International Studies.

5 Lissandra Paragassu, ”BRICS finance ministers make unified proposal for IMF reforms”, Reuters, 5 juli 2025.

6 Camila Bomfim, ”Brasil condicionou ampliação do Brics a apoio à reforma do Conselho de Segurança da ONU”, *g1*, 24 augusti 2023; Government of South Africa, ”XV BRICS Summit Johannesburg II Declaration: BRICS and Africa: Partnership for Mutually Accelerated Growth, Sustainable Development and Inclusive Multilateralism, 23 augusti 2023.

7 Ramos, Rocha och Zahreddine, ”A Agenda de Segurança Internacional no BRICS (2009–2019)”, 3.

En av Brasiliens främsta säkerhetspolitiska målsättningar är att skapa ett starkt försvar samt ett motståndskraftigt samhälle och ekonomi. Eftersom Brasilien inte hotas av någon extern statlig aktör, framhåller de försvarspolitiska dokumenten – det vill säga försvarspolitiken och försvarsstrategin – andra typer av hot, som organiserad brottslighet, den globala uppvärmningen och dess konsekvenser på klimatet och samhället, samt växande geopolitiska spänningar mellan världens stormakter.[8] Oron är att dessa hot kan begränsa landets suveränitet och strategiska autonomi. Den nationella försvarspolitiken (*Política Nacional de Defesa*, PND) definierar nationell säkerhet som ”tillståndet som möjliggör suveränitet och territoriell integritet [och] realiseringen av nationella intressen trots påtryckningar och hot oavsett vilken form dessa tar”.[9] Försvaret av Brasilien definieras som ”oskiljaktigt från landets utveckling”. PND förespråkar dessutom närmare relationer med länder som är teknologiskt mer avancerade än Brasilien för att höja försvarets förmågor. Den strategiska autonomin, utifrån ett brasilianskt perspektiv, bör således förstås som förmågan att föra en självständig och motståndskraftig politik, fri från yttre politiska och ekonomiska påtryckningar.

Ett fördjupat säkerhetssamarbete inom Brics skulle dessutom kunna skada Brasiliens redan väletablerade relationer till västländer, framför allt USA, men också Frankrike och Sverige.[10] De tre länderna bidrar till Brasiliens försvarsmaterielförsörjning och deltar i gemensamma militärövningar. I jämförelse har ytterst få övningar genomförts med och väldigt lite försvarsmateriel införskaffats från Kina och Ryssland.[11] Däremot har Brasilien närmare försvarspolitiska relationer med Sydafrika och Indien, med vilka Brasilien genomfört gemensamma militärövningar sedan 2008.[12] Även om relationerna med USA ibland har kantats av ideologiska och politiska spänningar så har de förblivit starka. Den första Trump-administrationen utnämnde exempelvis Brasilien till en *major non-Nato ally*, och Biden-administrationen uttryckte stöd för att peka ut Brasilien som en global Natopartner.[13] Relationerna störtdök dock under våren 2025, då den andra Trump-administrationen införde femtioprocentiga tullar på brasilianska varor och utlyste sanktioner mot en domare vid högsta domstolen. Men de återhämtade sig igen under hösten efter att Trump och Lula radade upp telefonsamtal och möten.[14]

Brasiliens starka säkerhetspolitiska band till USA innebär att Brasília sannolikt inte skulle acceptera att Brics rörde sig mot ett mer omfattande säkerhetspolitiskt samarbete. Det enda Brics-land som Brasilien i teorin skulle kunna tänka sig ett närmare säkerhetsfokuserat samarbete med är Sydafrika. Orsaken är de växande spänningarna mellan USA och Kina som kan få geopolitiska konsekvenser i Sydatlanten, en region som Brasilien uppfattar som strategisk viktig.[15] Utsikterna för en Brics-allians är således små utifrån Brasiliens perspektiv, men samarbeten är möjliga på specifika säkerhetspolitiska områden, som cybersäkerhet, organiserad brottslighet och kontraterrorism, samt inom FN:s säkerhetsråd, framförallt om de förbättrar Brasiliens internationella status.

Det är således föga överraskande att det är just inom områdena cybersäkerhet, organiserad brottslighet och kontraterrorism som Brics har gjort störst framsteg. Bland annat har Brics etablerat arbetsgrupper som tagit fram formuleringar inför toppmötena. Dessutom har arbetsgrupperna inom Brics ofta koordinerat mellan ländernas nationella säkerhetsrådgivare eller motsvarande.[16]

Trots framstegen tyder mycket på att Brasilien kommer att motsätta sig ett fördjupat samarbete på cyberområdet. För det första verkar inte cyberområdet vara en nationell politisk prioritet under Lula, och därmed vore det osannolikt att det skulle bli det på Brics-nivå.[17] För det andra dominerar Brasiliens försvarsmakt och försvarsmyndigheter politiken på cyberområdet tillsammans med kansliet för den nationella säkerhetsrådgivaren (*Gabinete de Segurança Institucional da Presidência da República,* GSI). Motsättningar mellan Lula-regeringen och högt uppsatta inom försvarsmakten

8 Ministério de defesa, ”Política nacional de defesa” & ”Estratégia nacional de defesa”, 2020

9 ”Política nacional de defesa” & ”Estratégia nacional de defesa”, 11.

10 Olivier Milland, *Brasiliens säkerhetspolitik: Stormaktsambitioner, strategisk autonomi och militär makt*, FOI-R--5589 --SE (Stockholm: FOI, 2024).

11 Han och Papa, ”Brazilian alliance perspectives: towards a BRICS development-security alliance?”, 1128; Milland, *Brasiliens säkerhetspolitik: Stormaktsambitioner, strategisk autonomi och militär makt*.

12 Han och Papa, ”Brazilian alliance perspectives: towards a BRICS development-security alliance?”.

13 Milland, *Brasiliens säkerhetspolitik: Stormaktsambitioner, strategisk autonomi och militär makt*.

14 Valerie Wirtschafter, ”An unexpected opening for US-Brazil tech cooperation”, Brookings Institution, 23 oktober 2025.

15 Han och Papa, ”Brazilian alliance perspectives: towards a BRICS development-security alliance?”, 1127.

16 Ramos, Rocha och Zahreddine, ”A Agenda de Segurança Internacional no BRICS (2009–2019)”, 9.

17 Joe Devanny och Russel Buchan, ”Brazil’s Cyber Strategy Under Lula: Not a Priority, but Progress is Possible”, augusti 2023, Working paper – Carnegie Endowment for International Peace, 1.

gör det tveksamt att regeringen mer aktivt skulle försöka att omformulera den brasilianska politiken.

## 3.2 Internets utveckling i Brasilien

Brasiliens första internetanslutning etablerades 1992 mellan akademiska institutioner i landet.[18] Tre år senare lanserades de första kommersiella anslutningarna och föreskrifterna. Utbyggnaden av internet kom bara några år efter återgången till demokrati 1988 och under en tid av omfattande infrastruktursatsningar, framför allt på vägnätet och telefonin. Flera statsägda telekombolag privatiserades, vilket sammanföll med en snabb ökning av telefonin, där hundratals små och medelstora företag etablerades.[19] På ungefär tio år ökade antalet användare av fast telefoni från 13 miljoner till 43 miljoner.[20] Vid mitten av 00-talet hade runt 180 miljoner mobiltelefoner registrerats för användning, vilket motsvarade en penetration på mer än 90 procent.[21] År 2025 hade antalet mobilabonnemang i Brasilien nått 210 miljoner.[22]

Även utbyggnaden av internet gick snabbt. I december 2024 uppskattades 89,4 procent av brasilianska hushåll ha tillgång till internet i hemmet, en ökning från 31,3 procent 2010, vilket var den senaste gången en liknande studie genomfördes.[23] Det finns dock stora skillnader inom landet, där städerna och industrinaven i de sydöstra delstaterna är de mest uppkopplade och de glesbefolkade norra och västra delarna av landet är mer fläckvist uppkopplade. Landets stora territorium, svårgenomträngliga regnskog och glesbefolkade områden utgör naturliga barriärer för internets utveckling.

Brasiliens anslutning till det internationella nätet sker framförallt genom undervattenskablar, som löper mellan Brasilien, andra sydamerikanska länder, USA, Europa och Afrika. År 2024 var landet anslutet till 18 undervattenskablar, varav åtta till USA, via fyra kabellandningspunkter i Brasilien.[24] Fyra undervattenskablar har också dragits genom Amazonasfloden. En kabel, som kopplar den brasilianska hamnstaden Fortaleza till Kameruns hamnstad Kribi, är byggd av Huawei.[25] Dock finns det ingen direktkoppling till Kina.

Merparten av landningsstationerna för de internationella undervattenskablarna ligger i just Fortaleza, huvudstaden i den nordöstra delstaten Ceará. Flera ligger också i de sydöstra delstaterna Minas Gerais, Rio de Janeiro och São Paulo (se Figur 3.1, nedan), där ungefär 41 procent av befolkningen bor.

Antalet datacenter, där företag lagrar, bearbetar och distribuerar data och datatrafik, i landet har också ökat markant. Totalt finns det 150 datacenter av varierande storlek och standard.[26] Merparten ligger i den sydöstra delen av landet (se Figur 3.1), men fler planeras även i de norra delarna. Då effekten av ett datacenter kan se väldigt annorlunda ut beroende på dess storlek kan energibehovet från datacentren vara ett hjälpsamt mått för att förstå storleksordningen på tillväxten. Mellan 2013 och 2023 ökade datacentrens energibehov från under 100 MW till mer än 770 MW. Tillväxt motsvarande ytterligare 510 MW var under konstruktion 2023 och datacenter för nära 400 MW i ökad energikonsumtion planeras de kommande åren, enligt den internationella fastighetsmäklaren och investeraren JLL.[27]

Utmaningarna med att bygga ut den fysiska infrastrukturen i de glesbefolkade delarna av landet förklarar troligen den snabba ökningen av satellitbaserade internetlösningar, framförallt från det amerikanska företaget Starlink. Sedan företaget fick sin licens 2022 har försäljningen tagit rejäl fart. På bara sex månader kom företaget att kontrollera 46 procent av den brasilianska marknaden, enligt en undersökning av den brasilianska myndigheten för telekommunikation, Anatel.[28] Detta

18 Rede Nacional de Pesquisa, ”Como a Rio-92 possibilitou a primeira rede de internet do país”, 2 juni 2022.

19 OECD, ”Chapter 2: Infrastructures for Brazil’s Digital Economy” i *OECD Reviews of Digital Transformation: Going Digital in Brazil*, 2020, 29–55, Paris: OECD Publishing. Manuel Gonzalo m.fl., ”5G Kick-off in India and Brazil: InterState Competition, National Systems of Innovation, and Catch-up implications for the Global South”, *Seoul Journal of Economics*, vol 36, nr..1, 53–78.

20 Timothy Power, ”Brazilian democracy as a late bloomer: Reevaluating the regime in the Cardoso-Lula era”, *Latin American Research Review*, vol. 45, nr. S1 (2010), 218–47.

21 Power, ”Brazilian democracy as a late bloomer: Reevaluating the regime in the Cardoso-Lula era”.

22 Teleco, ”Estatísticas de Celulares no Brasil”, uppdaterat 1 augusti 2025.

23 Mariana Tokarnia, ”Nove a cada dez brasileiros têm acesso à internet em casa”, Agência Brasil, 12 december 2024.

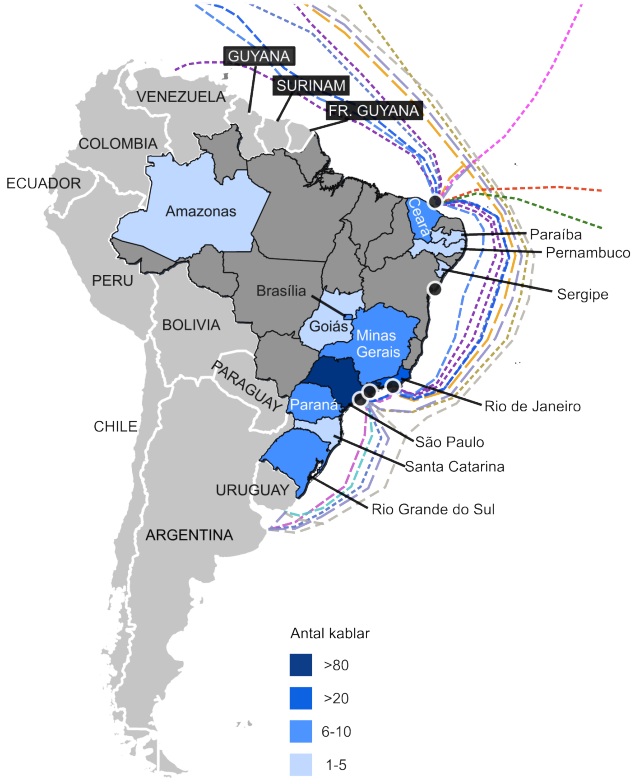
24 TeleGeography, ”The Submarine Cable Map”.

25 TeleGeography, ”The Submarine Cable Map”; Anna Gross, Alexandra Heal, Chris Campbell, Dan Clark, Ian Bott och Irene de la Torre Arenas, ”How the US is pushing China out of the internet’s plumbing”, *Financial Times*, 13 juni 2023; Liu Jia, Neusa Maria Pereira Bojikian, Aline Tedeschi, Rafael Ioris och Iury França, ”Strategic maneuvering in Brazil’s 5G deployment amidst United States-China technological rivalry”, 30 april 2024, *Revista Tempo do Mundo*, No.34, ss.419–451, Brasília: Institute of Applied Economic Research (Ipea).

26 Data Center Map,

27 JLL, ”Brazil Data Center Report: Brazil main markets 2023 outlook”, 2023.

28 Fabiane Ziolla Menezes, ”Tech Roundup: Starlink is the top satellite internet provider in Brazil”, The Brazilian Report, 29 juli 2024; Julio Wiziack, ”Empresa de Musk quase triplicou no país em menos de dois anos”, Folha de São Paulo, 10 april 2024.




**Figur 3.1** Författarens anpassning av data om Brasiliens internationella internetkablar och datacenter från TeleGeography – The Submarine Cable Map och Data Center Map.
**Källa:** TeleGeography och Data Center Map.

har lett till att Anatel övervägt att neka Starlink en utökad licens för dess andra generations satelliter för att motverka mono- eller duopol.

Även om satellituppkopplingarna löser vissa av de geografiska utmaningarna som nämnts ovan så utgör de också säkerhetsutmaningar för den brasilianska staten. I områden där satellituppkoppling dominerar verkar flera drogkarteller eller organiserade kriminella grupper som driver illegala gruvor. Dessa grupperingar har dragit nytta av de förbättrade uppkopplingarna på grund av låga krav vad gäller registrering och identifikation av användarna.[29]

Nittiotalets privatisering av den landbaserade infrastrukturen ledde till att stora utländska företag kom att dominera marknadssegmentet. Detta ledde till att andelen lokalägda företag förblev låg och därmed också investeringar inom brasiliansk forskning och utveckling på det digitala området.[30] Expansionstakten för digital infrastruktur har dock ökat de senaste åren. Enligt Organisationen för ekonomiskt samarbete och utveckling, OECD, var Brasiliens andel av telekommunikationsinvesteringar jämfört med inkomster 23,4 procent 2018, en bra bit över OECD-ländernas snitt på 15,7 procent.[31]

Idag är Brasilien ett av de ledande länderna i Latinamerika för informations- och kommunikationsteknik. Femte generationens mobiltelefoni (5G) lanserades formellt i november 2021 men utbyggnaden försenades.[32] Brasilien erbjuder uppkopplingar i fyra olika frekvensband: 700MHz, 3,5Ghz, 2,3GHz och 26 GHz.[33] Brasiliens 5G-utbyggnad utmärker sig i regionen eftersom regeringen krävde att de som vann upphandlingen skulle erbjuda *standalone*- (SA) uppkopplingar, det vill säga endast använda nybyggd 5G-teknik som

29 Rubens Valente, ”Elon Musk: Starlink resiste a mudra identificação de compradores de antenas na Amazônia”, Publica, 29 juli 2024.
30 Manuel Gonzalo m.fl, ”5G Kick-off in India and Brazil: InterState Competition, National Systems of Innovation, and Catch-up implications for the Global South”, 65.
31 OECD, ”Chapter 2: Infrastructures for Brazil’s Digital Economy”, 30.
32 Agência Nacional de Telecomunicações (Anatel), ”5G complea dois anos de implantação no Brasil”, 8 juli 2024; Pau Castells, James Joiner och Alejandro Adamowicz, ”5G in Latin America: Unleashing the potential”, GSMA Intelligence, juni 2023.
33 Conselho Administrativo de Defesa Econômica (CADES), ”Mercados de telecomunicações: Telefonia, acesso à internet e infraestrutura”, Cadernos do Cade, april 2023, 15.

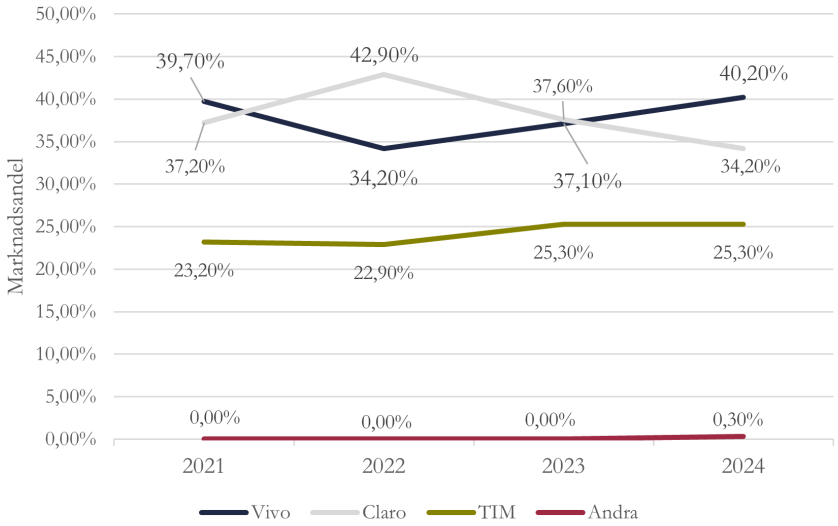
erbjuder snabbare uppkopplingar och lägre latens än tidigare generationens mobilnät (4G).[34] År 2023 rankades Brasilien som det femte snabbaste landet i världen mätt i median-nedladdningshastighet via 5G.[35] Två år efter att 5G-utbyggnaden påbörjades uppskattades att nästan 589 städer och ungefär 28 miljoner invånare ha tillgång till 5G-anpassade enhetsterminaler. Anatel planerar att alla kommuner i landet ska ha tillgång till 5G år 2029.[36]

## Brasiliens beroende av utländska företag

Även om det finns inhemsk produktion, så är Brasilien beroende av externa aktörer för sin hård- och mjukvaruutveckling. Nittiotalets privatisering och snabba infrastrukturutbyggnad samt Brasiliens stora marknadsstorlek innebar en uppsjö av utländska direktinvesteringar till landet, både genom företagsförvärv och nyinvesteringar. Detta ledde till att en den brasilianska telekommunikationsmarknaden domineras av flera utländska företag, som varierar lite mellan segmenten. Mobiloperatören med störst antal 5G användare är Vivo, ett dotterbolag till spanska Telefónica.[37] Tvåa är Claro, ett dotterbolag till Mexikos América Móbil. Den tredje största är TIM som kontrolleras av italienska Telecom Italia.

Endast ett företag med huvudsäte i Brasilien – Oi – fanns fram till 2021 med bland de fyra största mobiltelefoni- och bredbandsoperatörerna.[38] Dock tvingades företagskoncernen att sälja av bägge verksamhetsområdena på grund av en omstrukturering. Detta korrelerar med att både TIM och Vivos marknadsandelar ökade mellan 2023 och 2024.[39]

Ett liknande mönster gäller den landbaserade kommunikationsinfrastrukturen. Svenska Ericsson och finska Nokia är två ledande nätverksaktörer i landet. Den tredje stora aktören är kinesiska Huawei. Även om Ericsson och Nokia länge har dominerat den brasilianska marknaden har Huawei tagit allt större plats de senaste 25 åren. Idag finner man i varierande grad Huawei-utrustning i nästan alla brasilianska operatörers 3G- och 4G-nätverk.[40] Dock har de ovannämnda fyra största telekombolagen valt Ericsson eller Nokia som sin huvudsakliga leverantör av utrustning.[41] Som tidigare nämnts är Starlink den största aktören för satellituppkopplingar.




**Figur 3.2** Brasiliens marknad för 5G mobiltelefoni, 2021-24.
**Källa:** Teleco.com.br/5g_brasil.asp.

34 Pau Castells, James Joiner och Alejandro Adamowicz, ”5G in Latin America: Unleashing the potential”.
35 Anatel, ”5G completa dois anos de implantação no Brasil”.
36 Ibid.
37 Teleco, ”Market Share das Operadores de Celular 5G no Brasil”, senast uppdaterad 1 augusti 2025.
38 OECD, ”Chapter 2: Infrastructures for Brazil’s Digital Economy”; CADES, ”Mercados de telecomunicações ”, 21–22.
39 OECD, ”Chapter 2: Infrastructures for Brazil’s Digital Economy”; CADES, ”Mercados de telecomunicações”, 21
40 Manuel Gonzalo m.fl., ”5G Kick-off in India and Brazil: InterState Competition, National Systems of Innovation, and Catch-up implications for the Global South”, *Seoul Journal of Economics*, vol. 36, nr. 1 (2023), 53–78.
41 Manuel Gonzalo m.fl, ”5G Kick-off in India and Brazil: InterState Competition, National Systems of Innovation, and Catch-up implications for the Global South”, 68.

I takt med att Brasiliens infrastruktur har expanderat har antalet innovationshubbar och kompetensen på it-området ökat. Informationsplattformen StartupBlink, som varje år rankar startuplandskapen världen över, placerar Brasilien som det främsta innovationslandet i Latinamerika och det 27:e i världen.[42] Industrinavet São Paulo, där runt 60 procent av Brasiliens startupföretag är baserade, klassas som landets främsta innovationscentrum och landar på 23:e plats i världen (en plats före Stockholm).[43] Flera internationella it-företag, som Huawei och Amazon Web Services, har också investerat hundratals miljoner dollar i landet de senaste åren och mycket tyder på att mer är att vänta.[44] Huawei har exempelvis byggt två tillverkningsfabriker för mobiltelefoner, investerat i ett forsknings- och utvecklingscentrum och uppges planera ytterligare investeringar som datacenter.[45] Lulas inflytelserike utrikespolitiske rådgivare, Celso Amorim, har dessutom sagt att regeringen inte skulle motsätta sig en kinesisk halvledarfabrik i landet, även om Huaweis planer på en sådan fabrik inte har kommunicerats.[46] Dock för Brasilien också diskussioner med andra aktörer som EU och Malaysia om att stärka samarbetet kring halvledare.[47]

Att utveckla den inhemska tillverkningen av halvledare utgör för övrigt en viktig målsättning i de statliga satsningar på digitalisering och industriutveckling som pågått sedan september 2024. Bland annat vill Lula-administrationen utveckla inhemsk produktion av halvledare och datacenter och öka automatiseringen av företagsfunktioner.[48] Den 1 januari 2025 trädde en ny digitaliserings- och industrialiseringspolitik i kraft som syftar till att stärka incitamenten för företag att utöka sin digitalisering, med målsättningen att 90 procent av alla företag i Brasilien ska vara digitaliserade år 2033.[49] Regeringen har öronmärkt totalt 186 miljarder *reais* (cirka 336 miljarder svenska kronor) för programmet, varav 7 miljarder som årligen ska gå till att utveckla produktionen av halvledare genom hela värdekedjan. Denna satsning kommer även att få finansiellt stöd av den brasilianska utvecklingsbanken och innovationsfinansieringsmyndigheten Finep.[50]

Mjukvaruutvecklingen i landet domineras också till stor del av utländska aktörer. I Latinamerika utmärker sig Brasilien dock som ett centrum för mjukvaruutveckling, framförallt inom finans- och banksektorn.[51] Enligt den brasilianska föreningen för mjukvaruföretag, Abes, utvecklades endast en fjärdedel av mjukvaran som används i Brasilien lokalt 2023.[52] Även om det är en ökning från en femtedel 2020 så visar det på ett stort beroende av externa aktörer.

Brasilien har inga internationellt kända inhemska utvecklare av sociala medier eller sökmotorer. I linje med andra västländer dominerar amerikanskproducerade applikationer och sociala medier även om asiatiska applikationer har växt under senare år. Enligt den japanska konsultfirman Oosga var de tio mest använda sociala medierna 2022 i Brasilien WhatsApp, Instagram, Facebook, TikTok, Facebook Messenger, Kuaishou, Telegram, Pinterest och X (före detta Twitter).[53]

Flera operativsystem som bygger på Linux, har också utvecklats i landet eller av brasilianska programmerare, men det verkar inte finnas något renodlat brasilianskt operativsystem idag. Dock vittnar flera diskussionsforum och internetsidor om tidigare ambitioner att utveckla brasilianska operativsystem under 1980- och 90-talen. Senare försök att utveckla brasilianska operativsystem bygger nästan uteslutande på Linux.

42 StartupBlink, ”Global Startup Ecosystem Index: Top Countries”,

43 Ibid.

44 Reuters, ”Amazon’s AWS to invest $1.8 billion in Brazil through 2034”, 11 september 2024; Rodrigo Viga Gaier, ”Huawei eyes greater role in Brazil data center market”, Reuters, 9 juli 2025.

45 Angelica Mari, ”Huawei launches R&D center in Brazil”, 23 juni 2017, ZD Net; Igor Patrick, ”Huawei and ByteDance plan major investments in tech sectors in Brazil”, 17 juni 2025, *South China Morning Post*.

46 Anandira, Hana, ”Brazil strengthens China ties in boost to Huawei”, 14 april 2023, Mobile World Live,

47 Ministério da Ciencia, Tecnología e Inovação och EU, ”Strengthening EU-Brazil bilateral know-how of semiconductor sector technology and possibilities for cooperation on trade and R&D”, juli 2023; Malaysian Investment Development Authority, Brazil-Malaysia to set up joint development of IC design in 2025”, 1 december 2024.

48 Planalto, ”Chips, cloud and robotics : Brazil commits BRL 186.6 billion to drive industrial digitalization”, 11 september 2024

49 Planalto, ”Chips, cloud and robotics : Brazil commits BRL 186.6 billion to drive industrial digitalization”, 11 september 2024; FN:s konferens om handel och utvecklings Investment Policy Hub, ”Brazil – Extension and expansion of incentive regime for semiconductor industry”, 11 september 2024.

50 Planalto, ”Chips, cloud and robotics”.

51 International Institute for Strategic Studies, ”Cyber cababilities and national power – Volume 2”, 7 september 2023, 16.

52 Associação brasileira das empresas de software (ABES), *Mercado brasileiro de software 2024 : Panorama e tendências*, juli 2024.

53 Oosga, *Social Media in Brazil – 2023 Stats & Platform Trends*, 30 oktober 2023.

## 3.3 Internets tillstånd och framtid i Brasilien

Internets nutida tillstånd i Brasilien utmärker sig på olika sätt i de fysiska, logiska och cyberpersonalagren (se kapitel 2). Inom det *fysiska lagret* råder det få tekniska, politiska och juridiska begränsningar. Brasilien har en konkurrensutsatt och diversifierad telekommarknad för privata uppkopplingar, med tre aktörer som varit aktiva inom Brasiliens utbyggnad av tredje till femte generationens nätverk för mobiltelefoni. Huaweis möjliga deltagande i utbyggnaden av 5G genererade dock en intensiv debatt och omfattande amerikanska påtryckningar för att stänga ute företaget från Brasiliens spektrumauktion.[54]

Anatel meddelade dock i januari 2021 att alla leverantörer hade rätt att utveckla 5G-spektrumet i landet. Dock införde myndigheten krav på företagen som deltog, vilket i praktiken begränsade Huaweis möjligheter i vissa avseenden.[55] Kraven tros ha införts som en kompromisslösning för att undvika att specifikt förbjuda Huawei från spektrumauktionen, vilket kunde skada relationerna med Kina.[56] Bland annat krävde Anatel att 5G-utbyggnaden skulle innefatta ett allmänt och ett krypterat nätverk. Det senare ska bara användas av samhällskritiska federala myndigheter och militären.[57] För utbyggnaden av det skyddade nätverket krävde Anatel att endast utrustning som utvecklats, tillverkats och levererats av företag som uppfyller börsstandarder som är likvärdiga den brasilianska aktiemarknaden får användas.[58] Givet att Huawei, till skillnad från både Ericsson och Nokia, inte är börsnoterat innebär det rimligtvis att företaget inte uppfyller Anatels krav. I det offentliga nätverket krävde Anatel dessutom att utbyggnaden måste göras genom SA-uppkopplingar och att tidigare 4G-infrastruktur inte skulle nyttjas. Konsekvensen blev att kostnaden för att bygga ut 5G-nätverket drastiskt höjdes, eftersom SA-uppkopplingar kräver utbyggnad av ny infrastruktur och därmed mycket större investeringar. Samtidigt utlovade amerikanska myndigheter som Development Finance Corporation och den amerikanska export- och importbanken (EximBank) krediter på över 1 miljard amerikanska dollar till ”icke-kinesiska företag” för att bygga ut 5G-nätverket i Brasilien.[59]

Bakgrunden till beslutet var att USA aktivt försökte begränsa Huaweis och Kinas deltagande i utbyggnaden av 5G över hela världen, med även i Brasilien.[60] Frågan togs upp under flera besök mellan amerikanska och brasilianska representanter från militär och underrättelsetjänst under 2020. Samtidigt fördes en öppet Kinakritisk politik av den dåvarande presidenten Jair Bolsonaro och flera inom hans styrande krets, bland annat utrikesministern Ernesto Araújo och GSI-chefen Augusto Heleno Ribeiro Pereira. Dock höjdes flera röster emot politiken, bland annat från jordbrukssektorn och telekombolagen.[61] Den inflytelserika jordbrukslobbyn var orolig för att en bannlysning av Huawei skulle hota landets handelsrelationer med Kina – Brasiliens klart största konsument av jordbruksprodukter, framförallt sojabönor. Telekomsektorn varnade för orimligt höga kostnader eftersom det skulle innebära att även 3G- och 4G-teknologi som hade byggts av Huawei skulle behöva bytas ut.[62] Begränsningarna i spektrumauktionen blev således en kompromisslösning som i princip var öppen för alla spekulanter, men i praktiken införde restriktioner som rimligen var inriktade på Huawei. Trots begränsningarna hade Huawei i maj 2024 byggt 44 procent av landets dåvarande 5G-infrastruktur.[63]

Inom det *logiska lagret* (se kapitel 2) försöker myndigheterna framförallt att begränsa spridningen av skadlig programvara som kan användas för kriminella ändamål. Brasilien beskrivs återkommande som ett av de värst drabbade länderna i världen när det gäller cyberattacker. Finanssektorn har varit särskilt utsatt, men även myndigheter har blivit attackerade med omfattande konsekvenser. Under Covid-19 pandemins andra år slogs till exempel hälsodepartementets websidor ut i en *ransomware*-attack, utförd av hackergruppen Lapsus$ med bas i Brasilien och Storbritannien.

54 Oliver Steunkel, ”Huawei or Not? Brazil Faces a Key Geopolitical Choice”, *Americas Quarterly*, 30 juni 2020.

55 Ana Tereza Lopes Marra de Sousa m.fl., ”Entre o subserviência e o pragmatismo: o Brasil perante o 5G”, *Revista Oikos*, vol. 20, nr. 1 (2021).

56 Lopes Marra de Sousa m.fl., ”Entre o subserviência e o pragmatismo”; Jia m.fl., ”Strategic maneuvering in Brazil’s 5G deployment amidst United States-China technological rivalry”.

57 Agência Nacional de Telecomunicações, ”Entenda o Projeto de Rede Privativa de Comunicaçã da Administração Pública Federal”, 30 juli 2024, hämtad 12 augusti 2025; Andreia Verdélio, ”Leilão do 5G prevê criação de rede privativa para o governo federal”, Agência Brasil, 30 januari 2021.

58 Diário Oficial da União, ”Portaria No. 1.924/ SEI-MCOM, de 29 de janeiro de 2021”, 29 januari 2021.

59 Reuters, ”U.S. offers Brazil funding to buy 5G gear from Huawei rivals – diplomat”, 23 juni 2020; Ricardo Della Coletta och Julio Wiziack, ”Governo dos EUA promote crédito a teles brasileiras para não comprarem Huawei”, O Globo, 20 oktober 2020.

60 Jia m.fl., ”Strategic maneuvering in Brazil’s 5G deployment amidst United States-China technological rivalry”, 428–29.

61 Gonzalo m.fl, ”5G Kick-off in India and Brazil”, 67.

62 Julio Wiziack, ”Regras para leilão de 5G não restringem Huawei”, Folha de S. Paulo, 2 december 2020.

63 Simone Costa, ”Juntas, Ericsson e Huawei concentram 98% das vendas de antenas 5G no Brasil”, 21 maj 2024.

Attacken fördröjde implementeringen av nya reserekommendationer med en vecka.[64] Trots problemen visar statistik från Brasiliens CERT på att antalet attacker har fallit de senaste tio åren. Antalet rapporterade attacker mer än halverades från drygt 1 miljon 2014 till drygt 516 000 under 2024.[65] Medeltalet för attacker visar också på en tydlig nedåtgående trend mellan de första och sista femårsperioderna. Medelantalet för perioden 2014–2018 låg på 762 739, jämfört med medeltalet för 2019–2024 som låg på 521 610. Exakt hur mycket cyberkriminaliteten kostar brasilianska konsumenter och institutioner är oklart. Studier av olika cybersäkerhetsbolag varierar kraftigt i sina uppskattningar, från 10 miljarder amerikanska dollar årligen till 22 miljarder.[66]

*Cyberpersonalagret* och myndigheternas möjligheter att begränsa eller reglera det har blivit en central politisk fråga de senaste åren. Inte minst handlar det om myndigheternas försök till att begränsa spridningen av desinformation och främlingsfientlighet, framförallt från ytterhögergrupper, på sociala medier. Frågan som till en början handlade om att stärka den interna säkerheten har växt till att handla om att skydda den brasilianska demokratin och nationella suveräniteten. En faktor som ytterligare ökat frågans relevans är upproret som skedde den 8 januari 2023, då tusentals Bolsonaroanhängare stormade presidentpalatset, kongressen och högsta domstolen i huvudstaden Brasília. I september 2025 dömdes Bolsonaro och sju andra högt uppsatta från säkerhetsapparaten, däribland före detta försvarsministrar och en före detta GSI-chef, till mångåriga fängelsestraff för att ha planerat en statskupp och att med dödligt våld återta makten från president Lula två år tidigare.[67] Upproret i Brasília var, enligt åtalet, en del i en bredare plan där oroligheterna skulle utgöra en ursäkt till att utlysa undantagstillstånd.

Kopplingen till cyberpersonalagret är att upproret till stor del organiserades genom privata grupper på WhatsApp och drevs av en omfattande desinformationskampanj på flera sociala medier av Bolsonaro och hans allierade som felaktigt påstod att Lula hade vunnit presidentvalet 2022 genom omfattande valfusk. Problemet med desinformation var utbrett i Brasilien långt innan kuppförsöket, men blev allt mer problematiskt under Bolsonaros tid vid makten. Bland annat spred han och hans allierade desinformation under Covid-19 pandemin som till exempel resulterade i motstånd mot både hälsorestriktioner och vaccinationer. Domare från högsta domstolen och högsta valdomstolen har också hotats av grupper med kopplingar till Bolsonaro på grund av desinformation online.[68] Enligt en OECD-enkät i juni 2024 hade deltagare i Brasilien sämst förmåga att bedöma information på sociala medier (både sann och falsk information) jämfört med tjugo OECD-länder och Colombia.[69]

Förutom WhatsApp används även Telegram och X för spridning av desinformation i Brasilien. Myndigheterna har bestraffat alla tre plattformarna (eller deras moderbolag) på ett eller annat sätt de senaste åren. Antingen har plattformarna bötfällts eller så har åtkomsten till dem i Brasilien temporärt försvårats på grund av deras oförmögenhet eller vägran att moderera innehåll på ett, för myndigheterna, tillfredsställande sätt eller stänga av användarkonton som bryter mot deras egna användarvillkor och brasilianska lagar.[70]

Det mest högprofilerade fallet inträffade den 30 augusti 2024 då Brasiliens högsta domstol enhälligt beordrade X:s nedstängning i hela landet, på grund av att företaget inte hade följt tidigare nedstängningsordrar av individuella konton och betalat tidigare utfärdade dagsböter.[71] Dessutom hotade domstolen med ytterligare dagsböter på 50 000 reais (runt 95 000 kronor) för personer och organisationer som anslöt sig till plattformen via VPN-lösningar.[72] Nedstängningsordern kom efter att X inte tillsatt en juridisk representant inom 24 timmar som domstolen krävt. Microbloggplattformen förblev otillgänglig i Brasilien till den 8 oktober efter att företaget till slut gått med på att tillsätta den juridiska representanten, stänga ner de konton som myndigheterna

64 ”Brazil health ministry website hit by hackers, vaccination data targeted”, Reuters, 11 december 2021; Cyber Safety Review Board, ”Review of the attacks associated with Lapsus$ and related threat groups”, 24 juli 2023.

65 CERT.br, ”Incidentes Notificados ao CERT.br”.

66 Felipe Machado, ”Brasil perde US$ 10 bilhões por ano com cybercrime, diz McAfee”, 21 februari 2018, *Veja Negócios*; ”Hackers roubaram US$22 bi de usuários brasileiros em 2017”, 23 januari 2018; Devanny, Joe, Luiz Rogério Franco Goldini och Breno Pauli Medeiros, ”The rise of cyber power in Brazil”, *Revista Brasileiro de Política Internacional*, vol. 65, nr. 1 (2022).

67 Al Jazeera, ”Brazil Supreme Court sentences Bolsonaro to 27 years over coup plot”, 11 september 2025; Kathryn Armstrong, ”Bolsonaro ordered to start serving 27-year prison sentence for Brazil coup plot”, 26 november 2025; Milland, ”Brasiliens säkerhetspolitik”.

68 Global Freedom of Expression, ”The Case of the Brazil Fake News Inquiry”.

69 Molly Lesher, Hanna Pawelec och Mercedes Fogarassy, ”The OECD Truth Quest Survey: Methodology and Findings”, *OECD Digital Economy Papers*, juni 2024, nr.369, 24.

70 I WhatsApps fall har brasilianska myndigheter bötfällt moderbolaget Meta.

71 Supremo Tribunal Federal, ”STF confirma decisão que suspendou o X, antigo Twitter, em todo país”, 2 september 2024.

72 Ibid.

krävde och betalat böter till ett värde av 28,6 miljoner reais (runt 54 miljoner svenska kronor).[73]

Upptakten till nedstängningen karaktäriserades av växande spänningar mellan Elon Musk och högsta domstolsdomaren Alexandre de Moraes som utspelades offentligt på X. En utlösande faktor till dispyten var att de Moraes i april 2024 inkluderade Musk som misstänkt i en pågående utredning om så kallade ”digitala miliser” efter att X-chefen offentligt anklagat domaren för censur.[74] De ”digitala miliserna” är en term som används i Brasilien för att beskriva nätverk av individer som producerat, spridit och finansierat spridningen av desinformation som kopplats till statskuppsförsöket 2023. De Moraes uppges ha tolkat en kommentar som Musk gjort på plattformen som ett uppsåtligt försök att undergräva domstolens auktoritet.[75] Som svar hotade Musk med att öppna alla konton som blivit spärrade och uppmanade brasilianare att ansluta via VPN om X stängdes ner.[76]

Efterspelet till nedstängningen har också varit spänt och dessutom fått utrikespolitiska proportioner. I februari 2025 lämnade medieföretaget Trump Media & Technology Group (ägaren till Donald Trumps alternativa sociala medieplattform Truth Social) och videoplattformen Rumble in en stämningsansökan i USA mot de Moraes, som anklagades för att försöka censurera information i USA. Detta efter att de Moraes beordrat Rumble att stänga ner ett konto tillhörande en ”politisk dissident” eller riskera böter och nedstängning i Brasilien.[77] I juli införde Trump-administrationen 40-procentiga tullar, utöver de tullar som införts tidigare under året, på brasilianskt gods och utfärdade dessutom sanktioner mot de Moraes.[78] Besluten motiverades just med att de Moraes genom sina försök att begränsa desinformation i Brasilien hotat yttrandefriheten för amerikanska individer och företag i USA. Vita husets uttalande hävdade dessutom att de Moraes utredning av Bolsonaro utgjorde ”omotiverad politisk förföljning” av Bolsonaro och tydde på en ”kollaps av den brasilianska rättsstaten”.[79] Efter flera samtal mellan Lula och Trump under hösten 2025 har handelsspänningarna trappats ner och USA har lyft flera av de tullar som införts.[80]

Exakt var tvisterna kring 8 januari-upproret och Brasiliens försök att kontrollera cyberpersonalagret kommer att landa är oklart. Det som står klart är att kontroverserna belyst flera dilemman gällande Brasiliens cyberpersonalager, nationella suveränitet, demokrati och yttrandefrihet. Myndigheternas försök att begränsa spridningen av desinformation som anses utgöra en fara för staten ligger delvis bakom Brasiliens försämrade internationella anseende bland vissa organisationer. *Freedom On The Net*, den årliga rapport som tas fram av den amerikanska demokratifrämjande tankesmedjan Freedom House, rankar Brasiliens internet som delvis fritt.[81] Av totalt 72 länder vars frihet rankades 2024 låg Brasilien på 22:a plats globalt och 4:e plats i Latinamerika med en samlad poäng på 65 av 100 (där 100 är högst mått för frihet på Internet).[82] Brasiliens poäng har skiftat marginellt sedan 2019. Den största förändringen skedde 2016 då landet tappade tre poäng från 2015, det sista året då Brasiliens internet klassades som fritt.[83] Nedgraderingen skedde enligt Freedom House på grund av ett domslut som stängde ner WhatsApp tre gånger det året efter att företaget inte lämnat över användardata i en brottsutredning.[84] Tankesmedjan ansåg då att domslutet inte var proportionellt eftersom 100 miljoner användare i Brasilien förlorade tillgång till WhatsApp trots att appens moderbolag Facebook (numera Meta) förklarat att det inte lagrade den efterfrågade typen av data. Även följande upplagor av *Freedom on the Net* vittnar om Brasiliens utmaningar att balansera yttrandefriheten med riskerna som associeras med desinformation och domstolarnas överreaktioner.

73 André de Mello e Souza, ”Musk versus Moraes”, 19 december 2024, Development and Cooperation, hämtad 13 augusti 2025; Luciana Novaes Magalhes, ”Brazil’s top court says X paid pending fines to wrong bank”, 5 oktober 2024, hämtad 14 augusti 2025, *https://www.reuters.com/technology/musks-x-seek-resumption-brazil-service-fines-paid-sources-say-2024-10-04/*.

74 Global Freedom of Expression, ”Federal Supreme Court of Brazil v. Elon Musk and X”; Alex Rodrigues, ”Moraes inclui Elon Musk em inquérito das milícias digitais”, 8 april 2024, *Agência Brasil*.

75 Global Freedom of Expression, ”Federal Supreme Court of Brazil v. Elon Musk and X”.

76 Rodrigues, ”Moraes inclui Elon Musk em inquérito das milícias digitais”.

77 Truth Social använder Rumble för sitt videomaterial och en nedstängning av den senare plattformen hade fått konsekvenser för den förste; Ty Roush, ”Trump Media Sues Brazilian Judge – And Musk Foe – For Alleged Censorship”, *Forbes*, 19 februari 2025.

78 The White House, ”Addressing threats to the United States by the government of Brazil”, 30 juli 2025; U.S. Department of the Treasury, ”Treasury Sanctions Alexandre de Moraes”, 30 juli 2025. Michael Stott och Michael Pooler, ”US is planning new sanctions on Brazil, says Jair Bolsonaro’s son”, *Financial Times*, 11 augusti 2025, hämtad 2 augusti 2025.

79 The White House, ”Addressing threats to the United States by the government of Brazil”.

80 Reuters, ”Brazil’s Lula expects more US tariff cuts after call with Trump”, 3 december 2025.

81 Freedom House, ”Freedom On The Net Report 2024”, 16 oktober 2024.

82 Ibid.

83 Freedom House, ”Freedom on the Net 2015”, oktober 2015.

84 Freedom House, ”Freedom on the Net 2016”, november 2016.

## Drivkrafter och hot som förklarar Brasiliens agerande

Brasiliens motiv och fokus inom cyberpolitiken har utvecklats som ett resultat av den säkerhetspolitiska utvecklingen och myndigheternas uppfattning om hot och risker de senaste 15 åren. Enligt cyberforskarna Hurel och Lobato har cyberpolitiken utvecklats i tre faser.

Under den första fasen fokuserade Brasilien på hot från externa aktörer, speciellt cyberkrigföring och cyberspionage. Detta kom under en period med flera cyberattacker mot andra staters institutioner, bland annat ryska cyberattacker mot Estland och Georgien, 2007 respektive 2008, samt Stuxnetattacken på Irans kärnkraftverk i Natanz.[85] Brasilien ville reducera risken för incidenter förknippade med låg sannolikhet men med stor potentiell inverkan. Det fanns en oro att så kallade ”mega-event” som hölls i landet mellan 2012 och 2016 – däribland klimatkonferensen 2012 (Rio+20), Världsmästerskapet i fotboll 2014 och de Olympiska spelen 2016 – skulle öka risken för cyberattacker från andra stater. Edward Snowdens avslöjande av NSA:s avlyssningsaktivitet 2013 stärkte uppmärksamheten mot externa hot. Det ledde till att flera lagar antogs för att skydda brasilianska medborgares och myndigheters information och data.

Den andra fasen växte fram i skuggan av de makroekonomiska och sociopolitiska kriser som bröt ut i Brasilien efter priskraschen på naturresurser 2014 och uppdagandet av landets mest omfattande korruptionsupplägg: *Lava Jato*. Under den här fasen skiftade fokus alltmer från utländska hotaktörer till inhemska hot. Parallellt med att samhället polariserades växte nya fenomen fram genom den ökade användningen av sociala medier, som spridningen av desinformation, hacktivism och visselblåsande i cyberdomänen.[86] Trenden med desinformation har, som sagt, fått omfattande konsekvenser inom den brasilianska politiken.

Parallellt med dessa två faser växte cyberkriminaliteten i landet, framförallt brott med ekonomiska motiv. Brasilien är som nämnts ovan ett av världens mest utsatta länder för cyberkriminalitet. Detta har drivit fram en tredje fas som fokuserar mer på att förhindra, utreda och lagföra brott som genomförts inom cyberdomänen på olika sätt.

De tre faserna har färgat hur den brasilianska politiken har utformats de senaste 15–20 åren. Försvarsdepartementet och försvarsmakten har varit tongivande i den institutionella utvecklingen och gett den en militär inriktning.[87] Politiken kan delas in i tre fokusområden som stämmer överens med de tre faserna som nämnts ovan: cyberförsvar, cybersäkerhet och bekämpande av cyberkriminalitet. Det första fokuserar på militära hot och förmågor inom cyberdomänen. Det andra fokuserar på skyddet av den institutionella stabiliteten och politiska styrningen av cyberområdet. Det tredje fokuserar på att förebygga och bekämpa kriminalitet på cyberområdet.

Den nationella försvarspolitiken definierade redan 2008 cyberdomänen som en av tre strategiska domäner att stärka.[88] De andra två är kärnkrafts- och rymddomänerna. Två år senare etablerades det nationella centret för cyberförsvar (*Centro de Defesa Cibernética*, CDCiber) som 2014 införlivades som den operationella armen i det nationella cyberkommandot (*Commando de Defesa Cibernética*, ComDCiber).[89] Samma år etablerades den nationella cyberförsvarsskolan och den första cyberförsvarsdoktrinen publicerades.[90] Doktrinen definierade cyberförsvar som en kombination av offensiva, defensiva och inhämtande förmågor för att stärka det nationella försvaret.[91] Även om doktrinen nämner offensiva förmågor är det oklart hur utvecklade de är. Till exempel påstår Devanny, Goldoni och Medeiros, som har skrivit mycket om Brasiliens cyberpolitik, att det finns få tecken på att Brasilien använt sig av offensiva cyberoperationer.[92] Som en del i cyberförsvaret har Brasilien organiserat en årlig övning sedan 2018 – *Exercício Guardião* – som enligt den brasilianska försvarsmakten är den största cyberförsvarsövningen inom den södra hemisfären.[93] År 2024 deltog aktörer från 30 länder och 140 organisationer från försvaret, företagssektorn och civilsamhället.

85 Louise Marie Hurel och Luisa Cruz Lobato, ”Cyber security governance in Brazil: Keeping silos or building bridges?” i Scott N. Romaniuk och Mary Majikian (red.), *Routledge companion to global cyber-security strategy*, (Abingdon: Routledge, 2021).

86 Hurel och Cruz Lobato, ”Cyber security governance in Brazil”.

87 International Institute for Strategic Studies, ”Cyber capabilities and national power: Volume 2”, 7 september 2023.

88 Ministério de Defesa, ”Política Nacional de Defesa e Estratégia Nacional de Defesa”, 2012, 19.

89 Louise Marie Hurel, ”Mapping Cyber Policy in Latin America: The Brazilian Case”, Centro LATAM Digital, april 2023, 16.

90 Ibid.

91 Ministério de Defesa, Doutrina military de defesa cibernética, 2014.

92 Joe Devanny, Luiz Rogério Franco Goldini och Breno Pauli Medeiros, ”The rise of cyber power in Brazil”, 5.

93 Secretaria de Comunicação Social, ”Forças Armadas participam do maior exercício cibernético do Hemisfério Sul”, 19 oktober 2024.

Brasilien har också deltagit i Natos cybersäkerhetsövning *Locked Shields*.[94]

På cybersäkerhetsområdet är det motsvarigheten till kansliet för den nationella säkerhetsrådgivaren, GSI, som är den högsta instansen. GSI har ett brett mandat att skydda den institutionella säkerheten och stabiliteten, bland annat presidentens och vicepresidentens personliga säkerhet, kritisk infrastruktur, det brasilianska kärnkraftsprogrammet, samt cyber- och informationssäkerhet. Myndigheten domineras av militärer och inkluderar den brasilianska underrättelsetjänsten (*Agência brasileira de inteligência nacional,* ABIN) samt fyra sekretariat varav ett fokuserar på cybersäkerhet: *Secretaria de segurança da informação e cibernética,* SSIC).[95] SSIC är indelat i två departement, där det ena fokuserar på informationssäkerhet och det andra på cybersäkerhet. Sekretariatet, men även ABIN, ansvarar för frågor som rör cyber- och informationssäkerhet.[96] Precis som cyberförsvaret så stärktes GSI:s mandat över cybersäkerheten under 10-talet.[97] Bland annat har institutionen utökats med ett cyberincidenthanteringscenter (*Computer Security Incident Response Team*) och en styrgrupp för informationssäkerhet (*Comitê Gestor da Segurança da Informação*).

Departementet för rättvisa och offentlig säkerhet utgör den centrala institutionen för den tredje dimensionen av Brasiliens skydd av cyberdomänen: bekämpningen av cyberkriminalitet. Departementet har mandat att bekämpa allt som rör cyberkriminalitet, det vill säga brott som genomförs med hjälp av cyberdomänen men med tydliga konsekvenser utanför. Till dessa brott räknas bedrägerier och spridning av barnpornografi, eller brott som är beroende av de fysiska och logiska lagren av cyberdomänen, som exempelvis överbelastningsattacker, datastöld, eller *defacement*-attacker.[98]

Fokus ligger framförallt på att förebygga och utreda brott, bland annat genom att stärka polisens förmågor på delstatsnivå, samt på att samarbeta och koordinera med andra myndigheter på nationell och internationell nivå. På delstatsnivå har den civila polisstyrkan i 18 av 26 delstater etablerat specifika cyberenheter. Samtidigt har man etablerat ett sekretariat för integrerade insatser (*Secretaria de Operações Integrad*as).[99]

### Brasiliens hotbild

Brasiliens hotbild och säkerhetspolitiska analys är det som i stort formar dess cyberpolitik, även om landet inte står inför något existentiellt hot från någon extern stat. De främsta hoten är istället asymmetriska, som organiserad brottslighet och desinformation. Brasiliens intressen och säkerhetspolitiska mål om strategisk autonomi är också avgörande faktorer i hur landet förhåller sig till olika frågor på cyberområdet.

De asymmetriska hoten utgörs bland annat av olika typer av cyberattacker (överbelastningsattacker, nätfiske, riktat nätfiske och intrång i virtuella arbetsmiljöer). Dessa cyberattacker utförs av framförallt av inhemska organiserade kriminella grupper och nätverk men också alltmer av externa hotaktörer, både statliga och kriminella. Enligt Googles hotanalysgrupps data över cyberspionageattacker i Brasilien har 42 procent kopplingar till Kina, 31,7 procent till Nordkorea och 11,7 procent till Ryssland.[100] Hoten utgörs som sagt också av desinformation och hatbrott på internet (se avsnitt 3.3). Sådana hot kan påverka individers frihet, integritet och säkerhet samt det demokratiska styret.

## 3.4 Brasiliens ansats till Brics-samarbetet i cyberdomänen

Brasiliens syn på och målsättningar inom Brics kan bäst förstås mot bakgrund av landets ambition om högre status och strategisk autonomi. Sedan 00-talet har Brasilien försökt utmana rådande globala maktstrukturer genom att forma nya samarbetsorganisationer där Brasilien intar en ledande roll. Brics-samarbetet är det mest högprofilerade exemplet på global nivå, men Brasilien har även etablerat flera regionala samarbeten. Samtidigt som Brasilien utmanar rådande maktstrukturer försöker landet också balansera starka relationer med sina historiska partner i väst och relationer med framväxande makter som Kina och Ryssland. Detta innebär att Brasilien försöker upprätthålla principer om demokratiskt styre och mänskliga rättigheter parallellt med

94 Joe Devanny och Russel Buchan, ”Brazil’s Cyber Strategy Under Lula: Not a Priority, but Progress is Possible”, augusti 2023, Working paper – Carnegie Endowment for International Peace, 12.

95 Louise Marie Hurel, ”Mapping Cyber Policy in Latin America: The Brazilian Case”, Centro LATAM Digital, april 2023, 9.

96 Ibid.

97 Hurel, ”Mapping Cyber Policy in Latin America”, 12.

98 Defacement-attacker är dataintrång där förövaren gör ändringar i målets webbsidas innehåll eller utseende. Det kan påverka funktionaliteten på sidan men de används främst för att förmedla ett politiskt budskap (hacktivism) eller skada målets rykte (cyber-vandalism).

99 Louise Marie Hurel, ”Cybersecurity in Brazil: an analysis of the National Strategy”, Igarapé Institute, Strategic Paper, nr. 54, april 2021, 20.

100 Kristen Dennesen m.fl., ”Insights on Cyber Threats Targeting Users and Enterprises in Brazil”, Google’s Threat Analysis Group och Mandiant, 12 juni 2024.

fördjupade relationer med auktoritära stater. Brasiliens positionering inom Brics-samarbetet visar tydligt på denna balansakt.

Detsamma gäller Brasiliens cyberpolitik och ansats till globala cyberfrågor, där landet ibland beskrivs som en ”swing state”.[101] Som cyberforskarna Devanny och Russel noterar så har Brasilien de senaste tjugo åren främjat en flerpartsansats gällande den globala styrningen av internet, i motsats till Kina och Ryssland, som istället förespråkat att länders regeringar ska ha avgörande rollen.[102] Brasilien etablerade redan 1995 en styrkommitté för internet (*Comité Gestor da Internet*) som utgörs av representanter från statliga och privata sektorn, akademin och civilsamhället.[103] Samtidigt som Brasilien aktivt förespråkat skydd av mänskliga rättigheter motsatte sig landet länge att skriva på Budapestkonventionen mot cyberkriminalitet. Anledningen var att Brasilien uppfattade konventionen som ett europeiskt initiativ som Brasilien inte varit involverad i att ta fram och som på något vis inte kunde anses kunna ersätta andra konventioner som tagits fram inom FN. Brasilianska uttalanden från 2015 uttryckte istället en preferens för ett internationellt avtal inom FN-systemet. Brasilien ratificerade dock konventionen i november 2022 och den trädde i kraft i mars, året därpå.[104] Samtidigt är Brasilien också en av 25 medlemsländer i FN:s Group of Governmental Experts on Advancing responsible State behaviour in the Cyberspace in the context of international security, där även Kina, Ryssland och USA är medlemmar.[105]

I viss mån delar Brasilien Kinas och Rysslands oro över att västländer dominerar den globala styrningen av internet. NSA-skandalen tas regelbundet upp i debatten om vikten av att frigöra sig beroendet av USA. Samtidigt förespråkar Brasilien starkare skydd av sina medborgares data och integritet, och ställer högre krav på att data lagras och hanteras inom landets gränser. Brasiliens Allmänna dataskyddslag (*Lei Geral de Proteção de Dados*), som trädde i kraft 2020, tog exempelvis inspiration från EU:s dataskyddsförordning (känd som GDPR).[106] Även dess föregångare, Internetanvändningslagen (också känd som *Marco Civil da Internet*) förespråkade skydd av internetanvändares rättigheter och nätneutralitet.[107]

Brasilien kommer med största sannolikhet att fortsätta att driva en tvetydig politik inom Brics och andra internationella forum. Trots Brasiliens nära relationer till Kina och Ryssland så innebär dess nära säkerhetspolitiska relationer med västländer en bromskloss för hur långt och hur snabbt samarbetet inom Brics kan fördjupas. I och med att styrningen av internet i Brasilien till stor del domineras av försvarsmakten och säkerhetsapparaten, som har en nära relation till väst, finns det föga som talar för ett fördjupat Brics-samarbete på cyberområdet. Dessutom uppfattas cyberområdet inte som högprioriterat under den nuvarande Lula-administrationen.[108] Allt detta pekar på att Brasilien på sin höjd är öppet för ett begränsat samarbete inom Brics på cyberområdet.

## 3.5 Slutsatser

Det här kapitlet har tolkat Brasiliens ansats till Brics och fastslår att landet sannolikt kommer att motsätta sig en fördjupning av samarbetet på cyber-säkerhetsområdet över de kommande fem–tio åren. Brasilien ser framförallt Brics och dess medlemsländer som verktyg för att uppnå högre internationell status och värna om sina egna säkerhetspolitiska och geoekonomiska intressen. Brasiliens slutliga målsättning är att bli erkänd som en stormakt, vilket konkretiseras med ett permanent säte i FN:s säkerhetsråd. För att nå målsättningen försöker Brasilien skapa sig en ledarroll, inom San Francisco- och Bretton Woods-institutionerna men också inom nya forum som Brics. Detta gör Brasilien till en bro mellan två allt mer polariserade läger, där det ena domineras av USA och Europa, och det andra av Kina och Ryssland.

101 Devanny, Goldini och Medeiros, ”The rise of cyber power in Brazil”, 12.

102 Joe Devanny och Russel Buchan, ”Brazil’s Cyber Strategy Under Lula: Not a Priority, but Progress is Possible”, augusti 2023, Working paper – Carnegie Endowment for International Peace, 10.

103 Daniel Arnaudo, *Brazil, the Internet and the Digital Bill of Rights: Reviewing the State of Brazilian Internet Governance*, 2017, Rio de Janeiro: Instituto Igarapé.

104 Directorate of Legal Advice and Public International Law, Council of Europe, ”Notification of Accession”, 2 december 2022.

105 Ibid.

106 Daniel Opperman, ”Dimensions of Cybersecurity in Brazil” i Luca Belli cyberBRICS, 2021, 37; GDPR.eu, ”What is the LGPD? Brazil’s version of the GDPR”.

107 Nätneutralitet är en målsättning om att etablera ett öppet och rättvist internet, som bygger på principen om att alla internetleverantörer måste behandla all trafik likvärdigt. Det vill säga att de inte får begränsa eller bromsa ned informationsflöden, och att de inte får prioritera eller diskriminera vissa data över andra, oavsett avsändare. Joe Devanny och Russel Buchan, ”Brazil’s Cyber Strategy Under Lula: Not a Priority, but Progress is Possible”, 8.

108 Joe Devanny och Russel Buchan, ”Brazil’s Cyber Strategy Under Lula: Not a Priority, but Progress is Possible”.

Resultatet är en politik som kan tolkas som tvetydig eller ombytlig av externa aktörer.

Centrala förklaringar till tvetydigheten är Brasiliens säkerhetspolitiska målsättning om strategisk autonomi och utrikespolitiska tradition av alliansfrihet. Inrikespolitiska aktörers motstridiga prioriteringar spelar också en central roll för Brasiliens säkerhetspolitiska ställningstagande. Beslutet att inte specifikt stänga ute Huawei från landets 5G-utbyggnad är ett tydligt exempel på hur Brasilien tvingats balansera mellan utrikespolitiska målsättningar och geoekonomiska intressen. I det fallet balanserades presidentens ambition att stärka förhållandet med USA upp mot jordbrukslobbyns och telekombolagens oro över riskerna för motreaktioner från Kina – landets största handelspartner. Detsamma gäller utbyggnaden av fiberoptikkablar, vars diversifiering speglade den dåvarande regeringens oro över amerikanskt spionage efter NSA-läckan 2013.

För att minimera riskerna med handelsberoendet från Kina och för att stärka den brasilianska motståndskraften eftersträvar Brasilien att diversifiera sin ekonomi och utveckla en mer högteknologisk industri, genom teknologiöverföring från mer utvecklade länder i väst. Industrisatsningen genomförs till stor del tillsammans med den brasilianska försvarsmakten och producenter av försvarsmateriel samt västerländska partner vars försvarsindustrier är mer avancerade. Förhoppningen är att utvecklingen av högteknologiska försvarsföretag ska skapa tillväxtmöjligheter för andra högteknologiska industrier. Detta begränsar i praktiken hur mycket Brasilien kan fördjupa samarbetet med Kina och Ryssland och inom Brics-ramen.

Inom cyberdomänen finns det också flera aspekter som talar för detta. Här lyfts två aspekter. Den första är Brasiliens hotbild som domineras av interna och asymmetriska hot. Det misslyckade upproret och kuppförsöket den 8 januari 2023 kommer med största sannolikhet vara en central drivkraft och politisk fråga åtminstone under resten av Lulas mandatperiod. Fokus kommer därför fortsätta att vara på reglering av de logiska och cyberpersonalagren. Den andra viktiga aspekten kommer sannolikt att vara den fortsatta utbyggnaden av femte och sjätte generationens mobiltelefoni. Brasilien kommer med stor sannolikhet att fortsatt försöka balansera mellan riskerna och fördelarna med att tillåta kinesiska företag att bygga ut infrastrukturen. Även om länder som USA trappar upp sina påtryckningar för att begränsa kinesisk infrastrukturutbyggnad i Brasilien kommer ambitionen om teknologisk utveckling och kostnader fortsätta att väga tungt i beslutsfattandet.

# Referenser

Agência Nacional de Telecomunicações (Anatel), ”5G complea dois anos de implantação no Brasil”, 8 juli 2024, hämtad 3 oktober 2024. *https://www.gov.br/anatel/pt-br/assuntos/noticias/5g-completa-dois-anos-de-implantacao-no-brasil*.

Agência Nacional de Telecomunicações, ”Entenda o Projeto de Rede Privativa de Comunicaçã da Administração Pública Federal”, 30 juli 2024, hämtad 12 augusti 2025. *https://www.gov.br/anatel/pt-br/assuntos/noticias/entenda-o-projeto-de-rede-privativa-de-comunicacao-da-administracao-publica-federas*.

Agência Nacional de Telecomunicações (Anatel), ”Consulta pública No. 38”, hämtad 29 oktober 2024. *https://apps.anatel.gov.br/ParticipaAnatel/VisualizarTextoConsulta.aspx?TelaDeOrigem=2&ConsultaId=20257*.

*Al Jazeera*, ”Brazil Supreme Court sentences Bolsonaro to 27 years over coup plot”, 11 september 2025, hämtad 11 december 2025. *https://www.aljazeera.com/news/2025/9/11/brazils-bolsonaro-found-guilty-of-coup-plot-by-top-court*.

Armstrong, Kathryn, ”Bolsonaro ordered to start serving 27-year prison sentence for Brazil coup plot”, 26 november 2025, hämtad 11 december 2025. *https://www.bbc.com/news/articles/cr4dl19npv5o*.

Arnaudo, Daniel, *Brazil, the Internet and the Digital Bill of Rights: Reviewing the State of Brazilian Internet Governance*, 2017, Rio de Janeiro: Instituto Igarapé, hämtad 7 augusti 2025. *https://igarape.org.br/marcocivil/en/*.

Associação brasileira das empresas de software (ABES), *Mercado brasileiro de software 2021 : Panorama e tendências*, juni 2021.

Associação brasileira das empresas de software (ABES), *Mercado brasileiro de software 2024 : Panorama e tendências*, juli 2024.

Bomfim, Camila, ”Brasil condicionou ampliação do Brics a apoio à reforma do Conselho de Segurança da ONU”, *g1*, 24 augusti 2023, hämtad 2 oktober 2024. *https://g1.globo.com/politica/blog/camila-bomfim/post/2023/08/24/brasil-condicionou-ampliacao-do-brics-a-apoio-a-reforma-do-conselho-de-seguranca-da-onu.ghtml*.

Castells, Pau, James Joiner och Alejandro Adamowicz, ”5G in Latin America: Unleashing the potential”, GSMA Intelligence, juni 2023, hämtad 3 oktober 2024. *https://www.gsma.com/about-us/regions/latin-america/wp-content/uploads/2023/06/290623-5G-in-Latam-ENG.pdf*.

CERT.br, ”Incidentes Notificados ao CERT.br”, hämtad 8 augusti 2025, *https://stats.cert.br/incidentes/*.

Coletta, Ricardo, Della, och Julio Wiziack, ”Governo dos EUA promote crédito a teles brasileiras para não comprarem Huawei”, *O Globo*, 20 oktober 2020, hämtad 16 december 2024. *https://www.folhadelondrina.com.br/economia/governo-dos-eua-promete-credito-a-teles-brasileiras-para-nao-comprarem-huawei-3022268e.html?d=1*.

Conselho Administrativo de Defesa Econômica, ”Mercados de telecomunicações: Telefonia, acesso à internet e infraestrutura”, Cadernos do Cade, april 2023, hämtad 11 augusti 2025. *https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/estudos-economicos/cadernos-do-cade/Mercados-de-Telecomunicacoes_2023.pdf* .

Costa, Simone ”Juntas, Ericsson e Huawei concentram 98% das vendas de antenas 5G no Brasil”, Tele Síntese, 21 maj 2024, hämtad 16 december 2024. *https://telesintese.com.br/juntas-ericsson-e-huawei-concentram-98-das-vendas-de-antenas-5g-no-brasil/*.

Cyber Safety Review Board, ”Review of the attacks associated with Lapsus$ and related threat groups”, 24 juli 2023, hämtad 19 december 2024. *https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf*

Dennesen, Kristen m.fl., ”Insights on Cyber Threats Targeting Users and Enterprises in Brazil”, Google’s Threat Analysis Group och Mandiant, 12 June 2024, hämtad 12 december 2024. *https://cloud.google.com/blog/topics/threat-intelligence/cyber-threats-targeting-brazil/*.

Devanny, Joe, Luiz Rogério Franco Goldini och Breno Pauli Medeiros, ”The rise of cyber power in Brazil”, *Revista Brasileiro de Política Internacional*, Vol. 65, nr. 1 (2022), hämtad 19 december 2024. *https://doi.org/10.1590/0034-7329202200113*.

Devanny, Joe och Russel Buchan, ”Brazil’s Cyber Strategy Under Lula: Not a Priority, but Progress is Possible”, augusti 2023, Working paper – Carnegie Endowment for International Peace, hämtad 20 januari 2025. *https://carnegieendowment.org/research/2023/08/brazils-cyber-strategy-under-lula-not-a-priority-but-progress-is-possible?lang=en.*

Diário Oficial da União, ”Portaria No. 1.924/ SEI-MCOM, de 29 de janeiro de 2021”, 29 januari 2021, hämtad 13 augusti 2025. *https://www.in.gov.br/web/dou/-/portaria-n-1.924/sei-mcom-de-29-de-janeiro-de-2021-301396768.*

Council of Europe, Directorate of Legal Advice and Public International Law, ”Notification of Accession”, 2 december 2022, hämtad 8 augusti 2025. *https://rm.coe.int/0900001680a93e41*.

FN:s konferens om handel och utvecklings Investment Policy Hub, ”Brazil – Extension and expansion of incentive regime for semiconductor industry”, 11 september 2024, hämtad 24 oktober 2024. *https://investmentpolicy.unctad.org/investment-policy-monitor/measures/4814/brazil-extension-and-expansion-of-incentive-regime-for-semiconductor-industry*.

Fonseca Jr., Gelson, ”BRICS: Notes and questions” i *Brazil, BRICS and the international agenda*, red. José Vicente de Sá Pimentel, Brasília: Fundação Alexandre Gusmão, 19–45.

Fontenele Reis, Maria Edileuza, ”BRICS: Genesis and evolution” i *Brazil, BRICS and the international agenda*, red. José Vicente de Sá Pimentel, Brasília: Fundação Alexandre Gusmão, 47–71.

Freedom House. ”Freedom on the Net 2015”, Washington, DC: Freedom House, 2015, hämtad 7 augusti 2025, *https://freedomhouse.org/sites/default/files/FH_FOTN_2015Report.pdf*.

Freedom House, ”Freedom On The Net Report 2024”, Washington, DC: Freedom House, 2024, hämtad 28 oktober 2024, *https://freedomhouse.org/report/freedom-net/2024/struggle-trust-online*.

GDPR.eu, ”What is the LGPD? Brazil’s version of the GDPR”, hämtad 20 januari 2025. *https://gdpr.eu/gdpr-vs-lgpd/?cn-reloaded=1*.

Global Freedom of Expression, ”The Case of the Brazil Fake News Inquiry”, hämtad 13 augusti 2025. *https://globalfreedomofexpression.columbia.edu/cases/the-case-of-the-brazil-fake-news-inquiry/*.

Global Freedom of Expression, ”Federal Supreme Court of Brazil v. Elon Musk and X”, hämtad 13 augusti 2025. *https://globalfreedomofexpression.columbia.edu/cases/federal-supreme-court-of-brazil-v-elon-musk-and-x/?utm_source=chatgpt.com*.

Gonzalo, Manuel m.fl., ”5G Kick-off in India and Brazil: InterState Competition, National Systems of Innovation, and Catch-up implications for the Global South”, *Seoul Journal of Economics*, vol. 36, nr. 1 (2023), 53–78.

Government of South Africa, ”XV BRICS Summit Johannesburg II Declaration: BRICS and Africa: Partnership for Mutually Accelerated Growth, Sustainable Development and Inclusive Multilateralism, 23 augusti 2023, hämtad 6 augusti 2025. *https://www.gov.za/sites/default/files/speech_docs/Jhb%20II%20Declaration%2024%20August%202023.pdf*.

Gross, Anna Alexandra Heal, Chris Campbell, Dan Clark, Ian Bott och Irene de la Torre Arenas, ”How the US is pushing China out of the internet’s plumbing”, *Financial Times*, 13 juni 2023, hämtad 3 oktober 2024. *https://ig.ft.com/subsea-cables/*.

Han, Zhen och Mihaela Papa, ”Brazilian alliance perspectives: towards a BRICS development-security alliance?”, *Third World Quarterly*, 45, no.5, 1115–1136, hämtad 2 oktober 2024. *https://doi.org/10.1080/01436597.2022.2055539*.

Henrique, Layane, ”Inquérito das milícias digitais: Elon Musk x Alexandre de Moraes?”, Politize, 12 april 2024, hämtad 12 augusti 2025. *https://www.politize.com.br/inquerito-das-milicias-digitais/#o-que-e-o-inquerito-das-milicias-digitais*.

Hurel, Louise Marie och Luisa Cruz Lobato, ”Cyber security governance in Brazil: Keeping silos or building bridges?” i Scott N. Romaniuk och Mary Majikian, *Routledge companion to global cyber-security strategy* (red.), 2021. Abingdon: Routledge.

Hurel, Louise Marie, ”Cybersecurity in Brazil: an analysis of the National Strategy”, Igarapé Institute, Strategic Paper No.54, april 2021, hämtad 19 december 2024. *https://igarape.org.br/en/cybersecurity-in-brazil-an-analysis-of-the-national-strategy/*.

Hurel, Louise Marie ”Mapping Cyber Policy in Latin America: The Brazilian Case”, Centro LATAM Digital, april 2023, hämtad 19 december 2024. *https://centrolatam.digital/publicacion/mapping-cyber-policy-in-latin-america-the-brazilian-case/*.

International Institute for Strategic Studies, ”Cyber capabilities and national power: Volume 2”, 7 september 2023, hämtad 19 december 2024. *https://www.iiss.org/sv/research-paper/2023/09/cyber-capabilities-national-power-volume-2/*.

Jia, Liu, Neusa Maria Pereira Bojikian, Aline Tedeschi, Rafael Ioris och Iury França, ”Strategic maneuvering in Brazil’s 5G deployment amidst United States-China technological rivalry”, 30 april 2024, *Revista Tempo do Mundo*, nr. 34, 419–451, Brasília: Institute of Applied Economic Research (Ipea), hämtad 12 augusti 2025. *https://doi.org/10.38116/rtm34art16*.

Lesher, Molly, Hanna Pawelec och Mercedes Fogarassy, ”The OECD Truth Quest Survey: Methodology and Findings”, *OECD Digital Economy Papers*, juni 2024, nr. 369, 24, Paris: OECD Publishing, hämtad 17 december 2024. *https://www.oecd.org/en/publications/the-oecd-truth-quest-survey_92a94c0f-en.html*.

Lopes Marra de Sousa, Ana Tereza, m.fl., ”Entre o subserviência e o pragmatismo: o Brasil perante o 5G”, *Revista Oikos*, vol. 20, nr. 1 (2021), hämtad 11 april 2025. *https://revistas.ufrj.br/index.php/oikos/article/view/52051*.

Machado, Felipe, ”Brasil perde US$ 10 bilhões por ano com cybercrime, diz McAfee”, 21 februari 2018, *Veja Negócios*, hämtad 17 december 2024. *https://veja.abril.com.br/economia/brasil-perde-us-10-bilhoes-por-ano-com-cibercrime-diz-mcafee*.

Malaysian Investment Development Authority, Brazil-Malaysia to set up joint development of IC design in 2025”, 1 december 2024, hämtad 14 augusti 2025. *https://www.mida.gov.my/mida-news/brazil-malaysia-to-set-up-joint-development-on-ic-design-in-2025/*.

Mari, Angelica, ”Huawei launches R&D center in Brazil”, 23 juni 2017, ZD Net, hämtad 11 augusti 2025. *https://www.zdnet.com/article/huawei-launches-r-d-center-in-brazil/*.

Mello e Souza, André, de, ”Musk versus Moraes”, 19 december 2024, Development and Cooperation, hämtad 13 augusti 2025. *https://www.dandc.eu/en/article/musk-allows-social-media-platform-x-serve-right-wing-political-purposes-it-remains-be-seen*.

Milland, Olivier, *Brasiliens säkerhetspolitik: Stormaktsambitioner, strategisk autonomi och militär makt*, FOI-R--5589--SE, Stockholm: Totalförsvarets forskningsinstitut (FOI), 2024.

Ministério da Ciencia, Tecnología e Inovação och EU, ”Strengthening EU-Brazil bilateral know-how of semiconductor sector technology and possibilities for cooperation on trade and R&D”, juli 2023, hämtad 14 augusti 2025. *https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/lei-de-tics/Report_EUBRDialogues_SemiconductorsFINALEN.pdf*.

Ministério de Defesa, Doutrina military de defesa cibernética, 2014, hämtad 19 december 2024. *https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf*.

Novaes Magalhes, Luciana, ”Brazil’s top court says X paid pending fines to wrong bank”, Reuters, 5 oktober 2024, hämtad 14 augusti 2025. *https://www.reuters.com/technology/musks-x-seek-resumption-brazil-service-fines-paid-sources-say-2024-10-04/*.

OECD, ”Chapter 2: Infrastructures for Brazil’s Digital Economy” i *OECD Reviews of Digital Transformation: Going Digital in Brazil*, 2020, 29–55, Paris: OECD Publishing, hämtad 7 oktober 2024. *https://doi.org/10.1787/e9bf7f8a-en*.

Oosga, *Social Media in Brazil – 2023 Stats & Platform Trends*, 30 oktober 2023, hämtad 7 oktober 2024. *https://oosga.com/social-media/bra/*.

Opperman, Daniel ”Dimensions of Cybersecurity in Brazil” i Luca Belli cyberBRICS, 2021, s.35–49, Springer: Cham.

Paragassu, Lissandra, ”BRICS finance ministers make unified proposal for IMF reforms”, 5 juli 2025, Reuters, hämtad 6 augusti 2025. *https://www.reuters.com/world/china/brics-finance-ministers-make-unified-proposal-imf-reforms-2025-07-06/*.

Patrick, Igor, ”Huawei and ByteDance plan major investments in tech sectors in Brazil”, 17 juni 2025, *South China Morning Post*, hämtad 11 augusti 2025. *https://www.scmp.com/news/china/diplomacy/article/3314663/huawei-and-bytedance-plan-major-investments-tech-sectors-brazil*.

Planalto, ”Chips, cloud and robotics : Brazil commits BRL 186.6 billion to drive industrial digitalization”, 11 september 2024, hämtad 24 oktober 2024. *https://www.gov.br/planalto/en/latest-news/2024/09/chips-cloud-and-robotics-brazil-commits-brl-186-6-billion-to-drive-industrial-digitalization*.

Power, Timothy ”Brazilian democracy as a late bloomer: Reevaluating the regime in the Cardoso-Lula era”, *Latin American Research Review*, nr. S1, 218–47, hämtad 3 oktober 2024. *https://doi.org/10.1353/lar.2010.0034*.

Ramos, Leonardo, Pedro D. Rocha och Danny Zahreddine, ”A Agenda de Segurança Internacional no BRICS (2009-2019)”, *Dados* 64, no.3 (2021): 1-33, hämtad 2 oktober 2024. *https://doi.org/10.1590/dados.2021.64.3.245*.

Rede Nacional de Pesquisa, ”Como a Rio-92 possibilitou a primeira rede de internet do país”, 2 juni 2022, hämtad 3 oktober 2024. *https://www.rnp.br/noticias/como-rio-92-possibilitou-primeira-rede-de-internet-do-pais*.

Reuters, ”U.S. offers Brazil funding to buy 5G gear from Huawei rivals –diplomat”, 23 juni 2020, hämtad 16 december 2024. *https://www.reuters.com/article/markets/us/us-offers-brazil-funding-to-buy-5g-gear-from-huawei-rivals-diplomat-idUSL1N2E02LK/*.

Reuters, ”Brazil health ministry website hit by hackers, vaccination data targeted”, 11 december 2021, hämtad 19 december 2024. *https://www.reuters.com/technology/brazils-health-ministry-website-hit-by-hacker-attack-systems-down-2021-12-10/*.

Reuters, ”Amazon’s AWS to invest $1.8 billion in Brazil through 2034”, 11 september 2024, hämtad 10 december 2025. *https://www.reuters.com/technology/amazons-aws-unit-invest-18-bln-brazil-through-2034-2024-09-11/*.

Reuters, ”Brazil’s Lula expects more US tariff cuts after call with Trump”, 3 december 2025. *https://www.reuters.com/world/americas/brazils-lula-expects-more-us-tariff-cuts-after-call-with-trump-2025-12-03/* hämtad 10 december 2025.

Rodrigues, Alex, ”Moraes inclui Elon Musk em inquérito das milícias digitais”, 8 april 2024, Agência Brasil, hämtad 13 augusti 2025. *https://agenciabrasil.ebc.com.br/justica/noticia/2024-04/moraes-quer-inclusao-de-elon-musk-em-inquerito-das-milicias-digitais*.

Roush, Ty, ”Trump Media Sues Brazilian Judge – And Musk Foe – For Alleged Censorship”, *Forbes*, 19 februari 2025, *Forbes*, hämtad 13 augusti 2025. *https://www.forbes.com/sites/tylerroush/2025/02/19/trump-media-sues-brazilian-judge-and-musk-foe-for-alleged-censorship/*.

Secretaria de Comunicação Social, ”Forças Armadas participam do maior exercício cibernético do Hemisfério Sul”, 19 oktober 2024, hämtad 20 januari 2025. *https://www.gov.br/secom/pt-br/assuntos/noticias/2024/10/forcas-armadas-participam-do-maior-exercicio-cibernetico-do-hemisferio-sul*.

Steunkel, Oliver, ”Huawei or Not? Brazil Faces a Key Geopolitical Choice”, Americas Quarterly, 30 juni 2020, hämtad 11 augusti 2025. *https://www.americasquarterly.org/article/huawei-or-not-brazil-faces-a-key-geopolitical-choice/*.

Stott, Michael och Michael Pooler, ”US is planning new sanctions on Brazil, says Jair Bolsonaro’s son”, *Financial Times*, 11 augusti 2025, hämtad 2 augusti 2025. *https://www.ft.com/content/811e3add-7b3b-40bf-8698-bd18730f0869*.

Supremo Tribunal Federal, ”STF confirma decisão que suspendou o X, antigo Twitter, em todo país”, 2 september 2024, hämtad 13 augusti 2025. *https://noticias.stf.jus.br/postsnoticias/stf-confirma-decisao-que-suspendeu-o-x-antigo-twitter-em-todo-o-pais/*.

Teleco, ”Estatísticas de Celulares no Brasil”, uppdaterat 1 augusti 2025, hämtad 11 augusti 2025. *https://www.teleco.com.br/ncel.asp*.

Teleco, ”Market Share das Operadores de Celular 5G no Brasil”, senast uppdaterad 1 augusti 2025, hämtad 11 augusti 2025. *https://www.teleco.com.br/5g_brasil.asp*.

TeleGeography, ”The Submarine Cable Map”, hämtad 3 oktober 2024. *https://www.submarinecablemap.com/*.

Tokarnia, Mariana, ”Nove a cada dez brasileiros têm acesso à internet em casa”, Agência Brasil, 12 december 2024, hämtad 16 december 2024. *https://agenciabrasil.ebc.com.br/geral/noticia/2024-12/nove-cada-dez-brasileiros-tem-acesso-internet-em-casa*.

UNODC, ”Non-paper submitted by Brazil reflecting its views on the issue of cybercrime”, 18 maj 2015, hämtad 15 augusti 2025. *https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_24/ECN152015_CRP5_e_V1503408.pdf*.

U.S. Department of the Treasury, ”Treasury Sanctions Alexandre de Moraes”, 30 juli 2025, hämtad 12 augusti 2025. *https://home.treasury.gov/news/press-releases/sb0211*.

Valente, Rubens, ”Elon Musk: Starlink resiste a mudra identificação de compradores de antenas na Amazônia”, Agência Pública, 29 juli 2024, hämtad 29 oktober 2024. *https://apublica.org/2024/07/elon-musk-starlink-resiste-a-mudar-identificacao-de-compradores-de-antenas-na-amazonia/*.

*Veja Negócios,* ”Hackers roubaram US$22 bi de usuários brasileiros em 2017”, 23 januari 2018, hämtad 17 december 2024. *https://veja.abril.com.br/economia/hackers-roubaram-us-22-bi-de-usuarios-brasileiros-em-2017/*.

Verdélio, Andreia, ”Leilão do 5G prevê criação de rede privativa para o governo federal”, Agência Brasil, 30 januari 2021, hämtad 12 augusti 2025. *https://agenciabrasil.ebc.com.br/geral/noticia/2021-01/leilao-do-5g-preve-criacao-de-rede-privativa-para-o-governo-federal*.

Vestergaard, Jakob, ”Voice Reform in the World Bank”, 2010, Danish Institute of International Studies, hämtad 6 augusti 2025. *https://um.dk/en/-/media/websites/umen/danida/partnerships/research/2010/voice-reform-in-the-world-bank-2010.ashx*.

Viga Gaier, Rodrigo, ”Huawei eyes greater role in Brazil data center market”, Reuters, 9 juli 2025, hämtad 10 december 2025. *https://www.reuters.com/business/media-telecom/huawei-eyes-data-center-investments-brazil-says-executive-2025-07-09/*.

Weisbrot, Mark och Jake Johnston, *Voting Share Reform at the IMF: Will it Make a Difference?*, Washington, DC: Center for Economic and Policy Research, 2010, hämtad 2 oktober 2024. *https://cepr.net/images/stories/reports/IMF-voting-shares-2016-04.pdf*

White House, The, ”Addressing threats to the United States by the government of Brazil”, 30 juli 2025, hämtad 12 augusti 2025. *https://www.whitehouse.gov/presidential-actions/2025/07/addressing-threats-to-the-us/*.

Wirtschafter, Valerie, ”An unexpected opening for US-Brazil tech cooperation”, Brookings Institution, 23 oktober 2025, hämtad 5 februari 2026. *https://www.brookings.edu/articles/an-unexpected-opening-for-us-brazil-tech-cooperation/*

Wiziack, Julio, ”Regras para leilão de 5G não restringem Huawei”, *Folha de São Paulo*, 2 december 2020, hämtad 16 december 2024. *https://www1.folha.uol.com.br/mercado/2020/12/regras-para-leilao-de-5g-nao-restringem-huawei.shtml*.

Wiziack, Julio, ”Empresa de Musk quase triplicou no país em menos de dois anos”, *Folha de São Paulo*, 10 april 2024, hämtad 29 oktober 2024. *https://www1.folha.uol.com.br/colunas/painelsa/2024/04/empresa-de-musk-triplicou-no-pais-em-menos-de-dois-anos.shtml*.

Ziolla Menezes, Fabiane, ”Tech Roundup: Starlink is the top satellite internet provider in Brazil”, *The Brazilian Report*, 29 juli 2024, hämtad 29 oktober 2024. *https://brazilian.report/tech/2024/07/29/tech-roundup-starlink-satellite-internet/*

# 4. Ryssland – Brics som digital hävstång

*Carolina Vendil Pallin*

Ryssland var pådrivande för att Bric (och senare Brics) alls skapades som samarbetsplattform 2006. På president Vladimir Putins initiativ träffades ländernas förste vice utrikesministrar i samband med det årliga mötet i FN:s generalförsamling, något som blev startskottet för ett mer formaliserat samarbete.[1] Rysslands intentioner var till en början troligen mer inriktade på att utmana västs ledarskap på det ekonomiska området, medan Shanghaisamarbetet (Shanghai Cooperation Organization, SCO) fortfarande var ett viktigare format för säkerhetsfrågor.[2]

## 4.1 Rysslands relation med Brics

Brics fanns med redan 2009 som ett prioriterat samarbetsformat i ryska säkerhetspolitiska programdokument.[3] Den senaste Nationella säkerhetsstrategin kom i juli 2021. I den nämns Brics i det avslutande avsnittet som listar utrikespolitiska mål och då strax efter de organisationer som Ryssland bildat med före detta sovjetiska republiker samt Kina och Indien. Rysslands mål är enligt strategin från 2021 att stärka samarbete inom SCO och Brics liksom samverkan inom formatet RIC (Ryssland, Indien och Kina). Samarbete med t.ex. Europa kommer väsentligt längre ned i dokumentet.[4] Detta är relevant då ordningen i vilken länder nämns i dokumentet indikerar hur Ryssland vill att omvärlden ska tolka Moskvas geografiska prioritering. Landets Utrikespolitiska koncept från mars 2023 har ett avsnitt som behandlar hur Ryssland vill forma en ”rättvis och stabil världsordning” och anger att Brics är en av de kanaler Moskva vill använda. Brics förekommer också i ett avsnitt om ekonomiskt samarbete i konceptet.[5]

Bricssamarbetet har blivit viktigare i rysk politik i takt med att relationerna med väst har försämrats. Efter Rysslands andra invasion av Ukraina 2022 minskade utbytet med väst radikalt och Moskva försöker att kompensera för detta genom att bygga samarbeten med andra länder. Säkerhetsfrågor har också kommit mer i fokus än vad som var fallet inledningsvis. Brics har blivit viktigt som ett format för Ryssland att mildra effekterna av västliga sanktioner inom främst finanssektorn, teknologiutveckling och handel.[6]

När Ryssland tog över rollen som ordförande för Brics 2024 så skedde det under devisen ”Stärkt multilateralism för en rättvisare global utveckling och säkerhet”.[7] Ryssland hade dessutom en tydlig agenda att fortsatt använda Brics för att skapa mekanismer inom formatet för att undgå västs sanktioner. Under punkten ”Policy and Security” var ordförandeskapsagendan inriktad på att stärka det säkerhetspolitiska samarbetet, inklusive på informationssäkerhetsområdet. Ryska ordförandeskapet deklarerade som mål att ”etablera ett system för internationell informationssäkerhet för att förhindra och lösa konflikter i informationssfären och förhindra att den militariseras”.[8] Samtidigt är det tydligt att Moskva behöver driva denna politik med försiktighet inom Brics. Flera av Bricsländerna tvekar inför en politik som innebär ett entydigt avståndstagande från väst (se den här rapportens kapitel om Brasilien, Indien och Sydafrika). Det finns därmed gränser för

1 Cynthia Roberts, ”Russia’s BRICs Diplomacy”, *Polity*, vol. 42, nr. 1 (januari 2010): 1–13, 1–2. Se även Mark Raymond och Justin Sherman. ”Authoritarian multilateralism in the global cyber regime complex”, *Contemporary Security Policy*, vol. 45, nr. 1 (2023): 110–140, 125–127.

2 Roberts, ”Russia’s BRICs Diplomacy”. Se även Sergej Bojko, ”Problematika mezjdunarodnoj informatsionnoj bezopasnosti na plosjtjadjach SjOS v BRIKS”, *Mezjdunarodnaja zjizn*, nr. 1 (2019), och den jämförelse av sakfrågor inom Brics respektive SCO som två ryska forskare gjorde 2019, Maxim Bratersky och Georgy Kutyrev, ”BRICS and the Evolving Russia-India-China Security Agenda”, *Strategic Analysis*, vol. 43, nr. 6 (2019): 597–619.

3 Se §13 om bl.a. Bric i Rysslands nationella säkerhetsstrategi till 2020, presidentdekret nr. 537, 12 maj 2009, och §88 i Rysslands nationella säkerhetsstrategi, presidentdekret nr. 683, 31 december 2015.

4 Rysslands nationella säkerhetsstrategi, presidentdekret nr. 400, 2 juli 2021: §101:8.

5 Rysslands utrikespolitiska koncept, presidentdekret nr. 229, 31 mars 2023: §§19:4, 39:7.

6 Kirill Babajev, Andrej Kortunov m.fl., *Rossijsko-kitajskij dialog: model 2023*, RIAC, rapport nr. 87, (2023), 51–62.

7 Kreml, ”Obrasjtjenije Vladimira Putina v svjazi s natjalom predsedatelstva Rossii v BRIKS”, 1 januari 2024.

8 Jekaterina Korostovtseva, ”Jurij Usjakov: BRIKS na dele vyrazjajet interesy mirovogo bolsjinstva”, *TASS*, 5 mars 2024, se även Rysslands ordförandehemsida för Brics+ 2024, *https://brics-russia2024.ru/en/*.

hur långt Ryssland och Kina kan få med sig övriga länder.[9] Ryssland har också en fortsatt uppförsbacke för att återfå status internationellt, trots att landet stod värd för Bricstoppmötet i Kazan i oktober 2024.[10]

## 4.2 Internets utveckling i Ryssland

Rysslands internet utvecklades inledningsvis enligt den flerpartsmodell som gäller även för internet globalt. Universitet och företag i Ryssland skapade egna nätverk och enades om att överlåta hanteringen av domänen .ru till ett forskningsinstitut, RosNIIROS, 1994.[11] Detta gällde fram till 2001 då företaget RU-CENTER tog över ansvaret för att registrera domännamn inom domänen .ru. RU-CENTER fick ackreditering hos Internet Corporation for Assigned Names and Numbers (ICANN) 2003. Den ryska regeringen fick en egen representant i dess styrelse först 2005 och det var inte förrän 2011–2012 som den politiska ledningen på allvar började oroa sig för att den inte kunde kontrollera informationsspridningen på internet (efter den arabiska våren och demonstrationer på hemmaplan, se nedan).[12] Därefter har ryska myndigheter gradvis inskränkt friheten på internet. Freedom House rankade redan 2015 Ryssland som ”icke fritt” i sin rapport om *Freedom on the Net* och därefter har situationen försämrats ytterligare. Bland de 72 länder som Freedom House rankade 2024, låg Ryssland på femte plats från botten vad gäller friheten på internet (Kina och Myanmar låg sist).[13]

Internetanvändningen i Ryssland ökade som mest under en period mellan 2008 och 2014. Medan 2 procent uppgav att de använde internet varje dag eller ett par gånger i veckan 2001 och andelen sedan ökade till ungefär 10 procent under 2008, hade denna andel ökat till över 60 procent 2014. I mars 2024 låg siffran på strax över 80 procent och var som högst (98 procent) i åldersgruppen 18–25. Det är också den yngre andelen av befolkningen som i huvudsak får sin information från internet snarare än från tv, som var den ryska regeringens huvudsakliga propagandakanal. Unga använder också VPN[14] nästan dubbelt så ofta som övriga befolkningen och de noterar att de har problem att nå vissa digitala resurser ibland eller regelbundet (24 procent att jämföra med 12 procent för befolkningen som helhet).[15] Det framgår inte varför de resurser de försökte nå var otillgängliga. Överlag använder ryska befolkningen VPN för att få tillgång till blockerade mediaresurser och sociala medier och för att dessutom göra det anonymt.[16]

Med ökad repression och övervakning på internet har användningen av VPN-lösningar ökat i Ryssland. Redan under 2022 ökade efterfrågan rejält och under 2023 ökade antalet användare med 37 procent. Liksom tidigare är det framför allt unga och storstadsinvånare som använder VPN för att undvika myndigheternas blockeringar av webbsidor och tjänster på internet.[17] Allt fler i den ryska befolkningen får också sina nyheter från internet istället för från tv. På tio år har andelen som säger att de får sina nyheter från tv minskat från närmare 90 procent till strax över hälften av befolkningen som helhet. Bland unga personer (18–30 år) anger bara en fjärdedel att de får sina nyheter främst från tv.[18]

## 4.3 Rysslands cyberinfrastruktur

I Ryssland växte fram organiskt nerifrån i Ryssland snarare än utifrån statliga direktiv. Det har än idag konsekvenser för hur landets internet fungerar liksom för hur Rysslands fysiska och logiska lager (se kapitel 2) har utvecklats. Under 1990-talet upprättade ryska företag och universitet egna autonoma nätverk, inte sällan med egna ”gränsövergångar” eller uppkopplingar mot internet utanför Ryssland – uppkopplingar där internettrafik lämnar eller går in på ryskt geografiskt territorium. Sedan dess har Ryssland på olika sätt ökat kontrollen över internetknutpunkter, vilket följande avsnitt behandlar, liksom hur sjökablar kopplar ihop landet med omvärlden. Vidare har Ryssland genomfört en rad åtgärder som går under rubriken att skapa

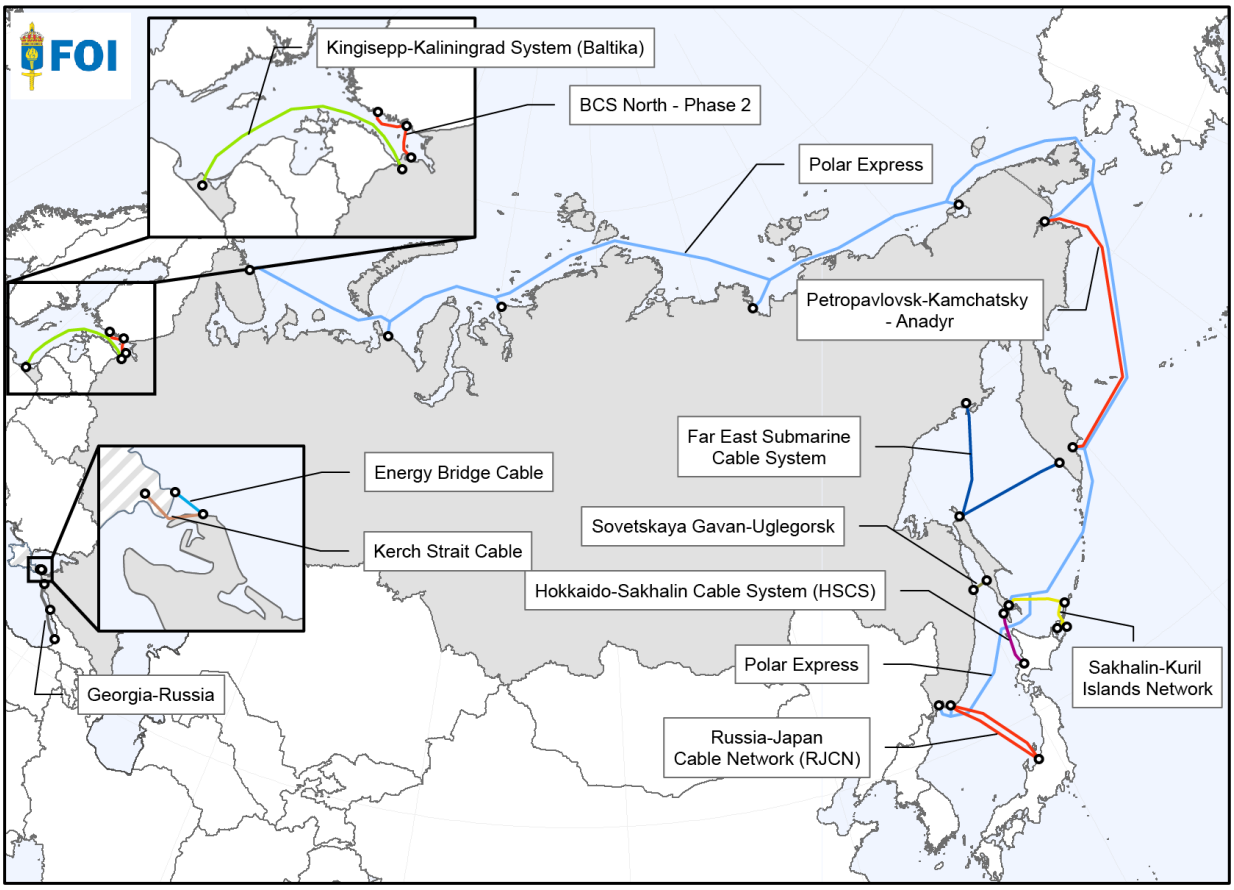
9 Andrej Kortunov, ”’Manifest novogo mirovogo porjadka’”, RIAC.
10 Janko Šćepanović, ”The 2024 BRICS Summit in Kazan”, PONARS Eurasia Policy Memo, nr. 917, november 2024.
11 Rossijskij nautjno-issledovatelskij institut razvittija obsjtjestvennych setei (Ryska vetenskapliga forskningsinstitutet för utveckling av samhälleliga nät).
12 Michael Yushenko, ”Internet governance in Russia”, i William J. Drake (red.), *The working group on Internet governance*: 10th Anniversary reflections, APC, 2015: 117–21. Se även Carolina Vendil Pallin, *Nyckelaktörerna för rysk cyberstrategi 2000–2020*, FOI-R--5025--SE, oktober 2020: 38ff.
13 Vendil Pallin, *Nyckelaktörerna för rysk cyberstratetgi 2000–2020,* 39–40. Freedom House, ”Freedom on the Net – 2024: Russia”.
14 Tjänster som försvårar spårning av din plats och avlyssning av trafik på Internet.
15 Levadacentrum. ”Auditorija polzovatelej internet, sotsialnych setej, messendzjerov i VPN-servisov”, 23 april 2024.
16 Adindex, ”Bolsjinstvo rossijan ispolzujut VPN dlja dostupa k sotssetami i SMI”, 6 december 2023.
17 Olga Mamikonjan, ”Kolitjestvo polzovatelej VPN v Rossii vyroslo potjti na 40 % v 2023 godu”, *Forbes*, 6 december 2023.
18 FOM. ”Novostnaja informatsija i televidenije”.

ett ”suveränt internet” samtidigt som rysk it-industri kontrolleras allt mer av statliga intressen. Tillsammans har det ökat regeringens kontroll över Rysslands cyberinfrastruktur.

## Internetknutpunkter och sjökablar

Ryssland har över 5 000 autonoma nätverk och strax under 40 internetknutpunkter (IXP:er) samt en decentraliserad marknad för internetoperatörer. Samtliga IXP:er utom en (BGP.Exchange - Moscow) domineras av medlemmar (autonoma system)[19] från Ryssland. En omstrukturering ägde rum i december 2021 som ledde till att den samlade överföringskapacitet i internetknutpunkter gick ner. Den sjönk ytterligare 2022, men i februari 2025 hade ryska IXP:er åter 2021 års överföringskapacitet.[20] På telekomområdet agerar landets dominerande telekombolag i praktiken som nivå-1-leverantörer och det är genom dem som trafiken når det globala internet.[21]

Rysk säkerhetspolitik ligger troligen också bakom hur regeringen har valt att prioritera läggandet av sjökablar. Av tiotalet sjökablar som ansluter till ryskt territorium ägs samtliga som lagts efter 2008 av ryska statskontrollerade bolag eller direkt av staten. Innan dess ingick Ryssland i gemensamma projekt med t.ex. Finland och Japan, men på senare år dominerar planer på sjökablar som anlöper endast Ryssland, varav jätteprojektet PolarExpress (12 650 km) är det bästa exemplet. Den är




**Figur 4.1** Befintliga och planerade sjökablar som ansluter till ryskt territorium.
**Källa:** TeleGeography, “Submarine Cable Map”, https://www.submarinecablemap.com/country/russia.

19 Inom ett autonomt system administreras ett antal routrar tillsammans och ”följer en gemensam policy för dirigering (*routing*)” av internettrafik i paket mellan varandra. Till exempel har internetoperatörer sina egna respektive autonoma system. De ansluter till en IXP, som kopplar samman autonoma system dels med det egentliga internet, dels med varandra så att meddelanden kan skickas lokalt för att spara tid utan att gå över globala internet. Computer Swedens it-ordlista, *https://it-ord.computersweden.se/ord/*.

20 Internet Society – Pulse, ”IXP Tracker – Russia”, data provided by Internet Society, *https://pulse.internetsociety.org/en/ixp-tracker/?country_code=RU&sort=-ixp_name*

21 Juho Niskanen, *Russia’s ICT-infrastructure and Its Development Prospects in the Near Future*, (Tammerfors, Finnish Defence Research Agency, 2023), 27–28.

planerad att ansluta i allra nordligaste västra Ryssland, längs hela Arktiskusten och ner till ryska Fjärran Östern när den är klar. Ursprungligen skulle projektet vara klart 2026, men 2025 stod det klart att inte ens första etappen var färdig och att bl.a. sanktionerna gjorde det osäkert när slutdatum kunde bli.[22] Tydliga säkerhetspolitiska överväganden ligger också bakom den kortaste sjökabeln som ansluter Ryssland till Kertj (46 km) och som lades direkt efter annekteringen av Krim. Samma övervägande gäller för den sjökabel som förbinder ryska Sachalin med Kurilerna, ögruppen som både Ryssland och Japan gör anspråk på (de Nordliga territorierna i japanskt språkbruk). Ryssland har också dragit en kabel genom Östersjön från Finska viken till Kaliningrad 2021 (se Figur 4.1).[23]

Fiberoptisk kabel finns framför allt i de områden där det finns en hög befolkningsdensitet, vilket främst är i de västra delarna, det europeiska Ryssland. Fiberdragningen tenderar dessutom att ligga längs med järnvägar. Det här innebär en utmaning för Ryssland när landet i framtiden står inför uppgiften att bygga nästa generations uppkoppling som både innebär ett behov av modernisering och av att täcka mer av landet, t.ex. hela vägnätet. Ryssland är även efter Sovjetunionens upplösning världens till ytan största land, med många mycket glest befolkade och otillgängliga områden. I sådana områden måste Ryssland förlita sig på satellituppkoppling inom den överskådliga framtiden eller en hybridlösning av satellit- och landburen mobiluppkoppling.[24]

En av de sårigaste frågorna för Ryssland att lösa ut är hur utbyggnaden av femte generationens (5G) internet ska ske. En anledning till detta är val av frekvenser. Försvarsministeriet och andra så kallade kraftministerier (som t.ex. den Federabal säkerhetstjänsten, FSB) vill inte släppa det som i Ryssland ofta benämns som det ”gyllene frekvensbandet”, området mellan 3,4 och 3,8 GHz. Anledningen till att det gyllene frekvensbandet är eftertraktat är dels att det innebär att färre basstationer behövs, dels att det redan finns ett ekosystem av utrustning för bandet. Istället hänvisar mobiloperatörerna till 4,4–4,9 GHz.[25] Ryska rymdmyndigheten, Roskosmos, har erbjudit sig att släppa 200 Mhz till 5G, med det löser inte dilemmat.[26] Ryssland kommer som ett resultat av detta att behöva fler basstationer och särskild utrustning för 5G på ”ryska” frekvenser, något som innebär stora investeringskostnader för mobiloperatörerna. Den ryska regeringens strategi för kommunikationsindustrin från 2023 nämner bara ett behov av att ”öka effektiviteten i styrningen och användandet av radiofrekvenser”.[27]

Vad gäller 5G ingår det också i den ryska importsubstitutionspolitiken att i möjligaste mån förlita sig på ryskproducerad utrustning. Ett antal ryska företag försöker få kontrakten och de statliga stöd som skulle vara förknippade med dessa. I handlingsplaner för digitala framtidsteknologier som togs fram 2019 var målsättningen att 10 procent av befolkningen skulle använda 5G 2024; i regeringens strategi från 2023 är målet istället att andelen ryska invånare med tillgång till 5G där de bor ska vara 10 procent 2030 och 30 procent 2035 i ett basscenario (i ett mer optimistiskt scenario: 25 procent år 2030 respektive 60 procent år 2035).[28] Sammantaget innebär detta ytterligare förseningar för Ryssland vad gäller att bygga ut 5G samt minskad lönsamhet för det näringsliv som förväntas stå för huvuddelen av kostnaden.

## Ett suveränt internet

Rysslands fysiska lager i form av bland annat IXP:er och sjökablar är således diversifierat vad gäller ägande, struktur och statlig kontroll som ett resultat av hur politiken ändrats från 1990 och framåt till dagens repressiva politik.[29] Att i efterhand bygga in kontroll över informationsspridning är en mer komplicerad uppgift än att etablera sådan redan när infrastrukturen först planeras. Ryssland har dock investerat avsevärda resurser i att kontrollera informationsspridningen inom det som Moskva definierar som ett ryskt segment av internet. Att etablera denna kontroll har också varit ett tydligt mål i officiella dokument som Informationssäkerhetsdoktrinen från 2016. Den lag som antogs 2019 – ofta refererad till som ”lagen om ett suveränt internet” – utgjorde ett viktigt

22 Pavel Korolev, ”’Poljarnyj ekspress’ vstal na pauzu”, *ComNews*, 14 mars 2025.

23 TeleGeography, ”Submarine Cable Map”.

24 Ryska regeringen, Strategi för att utveckla Ryska Federationens kommunikationsindustrin till 2035, 24 november 2023.

25 Janis Kluge, ”The future has to wait”, *Post-Soviet Affairs*, vol. 37, nr 5 (2021): 489–505. Se även Janis Kluge, *Russia's Transition to 5G: Stuck in a Regulatory Tug of War*, FPRI Report, August 2020.

26 Ilja Sizov, ”’Roskosmos’ podelitsia tjastotami”, *Kommersant*, 28 oktober 2024.

27 Ryska regeringen, Strategi för att utveckla Ryska Federationens kommunikationsindustrin till 2035.

28 Johan Engvall, Pär Gustafsson och Carolina Vendil Pallin, *Framtid med förhinder*, FOI-R--5204--SE, oktober 2021, 60–61 och Ryska regeringen, Strategi för att utveckla Ryska Federationens kommunikationsindustrin till 2035.

29 Amreesh Phokeer. ”How Isolated is the Russian Internet? Consequences of the war in Ukraine”, *Pulse*, 7 juni 2024. Se även Internet Society – Pulse, ”IXP Tracker – Russia”.

steg på vägen för att kontrollera vilken information som ryska medborgare har tillgång till. Trots retoriken om rysk suveränitet på internet var avsikten inte primärt att skapa möjligheter att helt skära av Rysslands uppkoppling mot globala internet. Själva kärnan i lagen utgjorde kravet att ryska internetoperatörer skulle tvingas installera teknisk utrustning som möjliggjorde övervakning och blockering av trafikpaket som passerade deras servrar. Dessutom skulle myndigheten Roskomnadzor ha befogenhet att ta över och dirigera trafiken på ett ryskt segment av internet och möjligheten att temporärt eller i vissa regioner stänga av viss trafik.

Trots att Ryssland utsattes för massiva cyberattacker efter invasionen av Ukraina använde Ryssland inte möjligheten att stänga ned trafiken.[30] De enda gångerna det har hänt har varit i samband med politiska protester och då endast regionalt och för en begränsad tid och vissa tjänster (t.ex. meddelandetjänsten Telegram eller WhatsApp, tjänster som hösten 2025 blockerades på bred front, se nedan).[31] Det stärker intrycket att det primära motivet bakom lagen om ett suveränt internet var att strypa fri tillgång till oberoende information för den inhemska befolkningen snarare än cybersäkerhetsskäl. Att fortsätta att bygga ut övervakning och blockering på internet, främst under Roskomnadzors egid, är också en av få civila poster i regeringens budget som fortsatt får finansiering trots de ökade kostnaderna som kriget mot Ukraina innebär för Ryssland.[32]

## Rysk it-industri

Att internet etablerades nerifrån och utan stor inblandning från ryska myndigheter var troligen också en bidragande orsak till att it-sektorns innovation och företagande utvecklades relativt dynamiskt jämfört med många andra näringslivssektorer. Ryssland var ett av få länder i världen som tidigt fick en egen version av Facebook – först i form av Odnoklassiki, senare i form av vKontakte. vKontakte ägs av det numera statskontrollerade företaget VK och är idag den viktigaste sociala medieplattformen i Ryssland. Sökmotorn Yandex klarade sig relativt väl i konkurrensen med globala Google och utvecklades till ett teknikbolag med egen forskning och utveckling på flera digitala framtidsområden. Därmed har Ryssland en rad inhemska lösningar inom det *logiska lagret* av cyberdomänen. Däremot var Ryssland mindre framgångsrikt vad gäller att utveckla egen hårdvara, elektroniska komponenter som t.ex. integrerade kretsar och även programvara.

Från och med cirka 2012 började också kontrollen även över it-industrin att hårdna i Ryssland. Till exempel tvingades Pavel Durov, en it-entreprenör som bland annat låg bakom vKontakte och senare tjänsten Telegram, att lämna Ryssland och sitt ägande av vKontakte under 2014.[33] Företaget Yandex, som utvecklades till ett av Rysslands ledande teknikföretag, hamnade också under växande politiskt tryck innan det slutligen delades upp och upphörde att vara den digitala teknologihubb som det tidigare varit.[34] Telegram, vKontakte och Odnoklassniki är fortfarande bland de mest populära applikationerna, medan YouTubes och Instagrams närvaro minskar i takt med att ryska myndigheter alltmer effektivt blockerar dessa applikationer. TikTok ökar snabbt i popularitet och WhatsApp har länge behållit platsen som den mest använda meddelandetjänsten tätt följd av Telegram.[35] I maj 2025 lanserade dock VK en ny meddelandetjänst, Max, som det snart blev klart var ämnad att ersätta WhatsApp. Putin angav redan den 4 juni att statliga myndigheter skulle stödja användandet av Max, som en ”rysk meddelandetjänst”.[36] Ett ryskt telefonnummer och statligt ID krävs för att registrera sig som användare samtidigt som Max kommer att vara en applikation där ryska medborgare kan använda statliga tjänster för alltifrån deklaration av skatt till att ansöka om körkort. Parallellt med en massiv kampanj för att få ryska medborgare att migrera till Max, blockerade den ansvariga myndigheten, Roskomnadzor, allt oftare WhatsApp och Telegram.[37]

Ryssland har också många framgångsrika it-säkerhetsföretag; bland de mest kända kan nämnas Kaspersky Lab och Group IB vilka båda etablerat sig även internationell marknad. Rysslands anfallskrig mot Ukraina 2022 drog dock effektivt undan mattan

30 Carolina Vendil Pallin, *Rysslands cyberberedskap på hemmaplan*, FOI-R--5611--SE, augusti 2024.

31 Till exempel stängde Ryssland ner Telegram och WhatsApp lokalt i Basjkortostan i samband med stora folkliga protester där i mitten av januari 2024.

32 CNews. ”Roskomnadzor polutjit milliardov, tjtoby usilit blokirovki zapresjennych sajtov”, 16 september 2024.

33 Carolina Vendil Pallin, ”Internet Control through ownership: the case of Russia”, *Post-Soviet Affairs*, vol. 33, nr. 1 (2017), 16–33.

34 Vendil Pallin, *Nyckelaktörerna för rysk cyberstrategi*, 48ff. Se även Daria Dergacheva, ”The limits of compromise”, *Russia.Post*, 23 juni 2022.

35 Levadacentrum, ”Kanaly polutjenija informatsii, sotsialnyje seti i messendzjery”, 11 oktober 2024.

36 ”Sovesjtjanije s tjlenami pravitelstva”, Kremls hemsida, 4 juni 2025.

37 Ksenia Elzes, ”Everything you need to know about Max, Russia’s state-backed answer to Whatsapp”, *The Moscow Times*, 28 August 2025.

för dessa företag på den internationella marknaden. Samtidigt ökade efterfrågan på deras tjänster inne i Ryssland när företag där inte längre kunde använda västliga säkerhetslösningar på grund av sanktioner och att västliga företag lämnade den ryska marknaden.[38]

Att utveckla landets nationella it-industri nämns som ett av de prioriterade målen i landets Informationssäkerhetsdoktrin från 2016. Rysslands beroende av utländsk import på området är definierat som en säkerhetsrisk och innebär att ”vissa länder” kan använda sin teknologiska dominans i informationssfären.[39] Att ersätta importen med inhemsk produktion har dock visat sig svårt för Ryssland, trots en rad olika program och initiativ på området.

Den 24 februari 2022 när Ryssland anföll Ukraina, använde t.o.m. ryska myndigheter fortfarande västerländsk programvara och ofta också it-säkerhetslösningar som köpts in från väst. Detsamma gällde hårdvara – alltifrån servrar och kablar till mobiltelefoner importerades både från väst och från Kina.[40] De exempel på rysk produktion som existerade var som regel beroende av komponenter som importerades från utlandet. Underleverantörer av såväl hårdvara som programvara kom från utlandet; konsultbolag belägna utanför Ryssland levererade it-tjänster och ryska it-experter arbetade för internationella företag. För Ryssland innebar detta plötsligt en säkerhetsrisk. Dels utsattes landet för en våg av it-attacker, dels kunde många företag, som nämnts ovan, inte längre uppdatera sitt it-skydd samtidigt som västliga företag lämnade landet och sanktioner snabbt skapade nya problem.

Ytterligare en försvårande omständighet var bristen på personal inom it-sektorn. Den var betydande redan före februari 2022 och blev än mer besvärande när en våg av kvalificerade experter lämnade landet i och med att kriget mot Ukraina inleddes. Vissa bodde redan utomlands och arbetade på distans, vissa arbetade för västliga företag och flyttade med dem när de lämnade Ryssland. En andra våg av unga män, varav vissa inom it-branschen, lämnade landet när Moskva utlyste en partiell militär mobilisering i september 2022.[41]

Ryssland har tacklat dessa problem dels genom att försöka påskynda inhemsk utveckling av alltifrån hårdvara till operativsystem och programvara, dels genom att öka importen från främst Kina och dels genom att kringgå sanktionerna. I första hand är målet att ersätta västlig programvara inom statliga och regionala myndigheter och statsägda företag. Ryssland har också försökt att locka hem kvalificerad it-personal. När it-attacker avlöste varandra efter februari 2022 började också distansarbete från utlandet anses i Ryssland som en potentiell säkerhetsrisk. Det fick företag som VK att kräva att personal flyttade tillbaka till Ryssland för att få behålla jobbet. Vidare har Ryssland vidtagit åtgärder för att öka genomströmningen i utbildningar inom it-branschen och utlovat frisedel från mobilisering för it-personal.[42]

Att öka inhemsk tillverkning av hårdvara och elektroniska komponenter har visat sig fortsatt svårt. Ryssland har jämfört med Kina en mycket mindre inhemsk marknad vilket minskar skalfördelar i produktionen samtidigt som de har kommit för sent till den internationella marknaden för att vinna andelar där.[43] Utmaningarna för Ryssland är än större efter februari 2022. Landet har i praktiken avhänt sig möjligheten att balansera sitt importberoende mellan väst och Kina. Landets it-industri är avskuret från innovation, marknader och möjligheter att få tekniköverföring från väst i form av direktinvesteringar och forskningssamarbeten. Utvecklingen av artificiell intelligens (AI) är ett område där Ryssland på olika sätt vill stimulera egen forskning och utveckling för att inte hamna efter globalt. Landet antog redan 2019 en AI-strategi och AI var ett av de digitala teknikområden som blev föremål för en särskild satsning samma år.[44] I februari 2024 antog Putin genom ett presidentdekret dessutom en uppdatering av AI-strategin, som bland annat innehöll ett längre tillägg om vikten av internationellt AI-samarbete, t.ex. inom ramen för Brics.[45] Att öka samarbetet inom Brics för att minska effekterna av västliga sanktioner har blivit viktigare än någonsin tidigare för Ryssland.

38 Vendil Pallin, *Rysslands cyberberedskap på hemmaplan*.

39 Rysslands informationssäkerhetsdoktrin, presidentdekret nr. 646, 5 december 2016, §§8:v, 17, 19, 25–27.

40 Elina Sinkkonen och Jussi Lassila, ”Digital Autoritarianism and Technological Cooperation in Sino-Rusian Relations” i *Russia-China Relations : Emerging Alliance or Eternal Rivals?* red. Sarah Kirchberger, Svenja Sinjen och Nils Wörmer (Cham.: Springer, 2000), 165–84.

41 Vendil Pallin, *Rysslands cyberberedskap på hemmaplan*.

42 Vendil Pallin, *Rysslands cyberberedskap på hemmaplan*.

43 Engvall, Gustafsson och Vendil Pallin. *Framtid med förhinder*, 48–50.

44 ”O razvitii iskusstvennogo intellekta v Rossijskom Federatsii”, presidentdekret nr. 490, 10 oktober 2019. Se även Anna Nadibaidze, ”Russia’s Drive for AI: Do Deeds Match the Words?”, *The Washington Quarterly*, vol. 47, nr. 4 (2024), 137–54 samt Engvall, Gustafsson och Vendil Pallin. *Framtid med förhinder*, 51–54.

45 Presidentdekret nr. 124, 15 februari 2024, §51:13.

## 4.4 Ryska initiativ inom Brics på cyberområdet

Bricssamarbetet utgjorde redan före 2022 ett sätt för Ryssland att öka sin prestige internationellt, men också ett forum för att driva sakfrågor, som t.ex. att få till stånd ett avtal i FN om internationell informationssäkerhet.[46] Ett konceptpapper från 2013 för Rysslands deltagande i Bricsformatet anger samarbete inom området internationell informationssäkerhet som ett av åtta säkerhetspolitiska mål för Ryssland. Även målet att skapa en ”gemensam informationssfär” inom Brics nämns, men då endast radio och tv liksom att Ryssland avser att skapa en tidskrift som kommer ut regelbundet och behandlar Brics verksamhet.[47] Brics nämndes dessutom som ett viktigt format för att driva rysk syn på hur ett system för internationell informationssäkerhet skulle utvecklas internationellt i ett dokument utgivet av Försvarsministeriet redan 2011 och i ett om rysk politik internationella informationssfären 2013.[48] I ett tidigt skede låg därmed tyngdpunkten i de ryska ambitionerna på samarbete inom den icke-digitala informationssfären, men också på Rysslands ambition att få till stånd ett internationellt avtal om informationssäkerhet i FN. Däremot nämndes inte Brics i Informationssäkerhetsdoktrinen som kom 2016.

### Inom Brics

Det dröjde också innan Ryssland fick igenom något konkret samarbete inom it-området inom Brics. Efter Edward Snowdens avslöjande om USA:s avlyssningsprogram 2013 torde dock Bricsländerna ha varit mer benägna att åtminstone börja diskussioner om sin cybersäkerhet och om samarbete på området. Under sitt ordförandeskap i Brics 2015 förde Ryssland fram tankar om ett fördjupat samarbete inom informations- och kommunikationsteknik (IKT). Redan året innan hade den ryska kommunikationsministern, Nikolaj Nikiforov, noterat på en inhemsk konferens att hälften av jordens befolkning bodde i Bricsländerna och att det där, enligt honom, fanns en efterfrågan på oberoende programvara: ”Ryssland borde i nära samarbete med administrationerna för samband och it i dessa länder inleda arbetet med att skapa lösningar vad gäller programvara inte bara för sin egen del utan för dessa i storlek betydande marknader.”[49] Inför Bricstoppmötet 2015 i Ufa besökte också Nikiforov samtliga Bricsländer och diskuterade då bl.a. gemensam utveckling av ”kritiskt viktig” programvara och av mikroelektronik.[50]

Punkt 33 i Ufa-deklarationen under det ryska ordförandeskapet 2015 tar upp informations- och kommunikationsteknologiers viktiga roll och att internet bör styras genom en ”öppen och demokratisk process”. På det stora hela är dock texten allmänt hållen. Samma år skapades en expertarbetsgrupp för IKT, som skulle träffas regelbundet. En jämförelse mellan den kommuniké som gick ut från ryska UD efter expertgruppens första möte och det sjätte mötet som ägde rum under Rysslands nästa ordförandeskap 2020 ger dock intryck av att länderna inte har lyckats ena sig om något annat än relativt allmänna skrivningar.[51] Ryska analytiker framhåller också att informationssäkerhet är en av komponenterna i Brics antiterrorstrategi från 2020. Ryssland var pådrivande även här för att informationssäkerhet skulle inkluderas,[52] men det finns frågetecken kring hur mycket reellt samarbete skrivningarna resulterade i.

Den 16–18 maj 2023 ägde det nionde mötet rum i den arbetsgrupp för säkerhet inom IKT-området som etablerades inom Brics 2015. En allmänt hållen kommuniké noterade att ”viktiga steg hade tagits” för ett samarbete mellan ”kompetenta organ” (vanligen en rysk omskrivning för underrättelse- och säkerhetstjänster) för att bekämpa it-attacker.[53] Som nämnts i inledningskapitlet föreslog en dumaledamot till och med att Ryssland skulle förmå länderna inom Brics+ att inleda bildandet av ett eget internet, ett som var oavhängigt av väst.[54] Något sådant förslag verkar dock inte ens ha kommit

46 A. A. Sergunin, ”Russia’s Strategies towards BRICS”, *Vestnik RUDN. International Relations*, vol. 20, nr. 3 (2020), 534–42.

47 ”Kontseptsija utjastija Rossijskoj Federatsii v obedinenii BRIKS”, antagen av Rysslands president, 21 mars 2013, §16:g och 30:z.

48 Se § 3:1 i Försvarsministeriet,”Kontseptualnyje vzgljady na dejatelnost vooruzjennych sil Rossjiskoj Federatsii v informatsionnom postranstve”; ”Gunderna för Ryska Federationens politik i informationssäkerhetsdomänen till 2020”, antagen med presidentorder nr. 1753, 24 juli 2013.

49 *ComNews*, ”IKT dlja BRIKS”, 13 juli 2015.

50 Ibid.

51 Ryska utrikesdepartementet, ”Pressmeddelande nr. 1229–19–06–2015, 19 juni 2015 respektive” Pressmeddelande nr. 1301–28–08–2020, 28 augusti 2020.

52 Aleksandr Ignatov och Jelena Zinoveva, ”’Tsifrovoj suverenitet’ v povestke obedinenija BRIKS”. RIAC, 24 januari 2024.

53 Ryska UD, ”O 9-m zasedanii Rabotjej gruppy BRIKS po voprosam bezopasnosti v sfere ispolzovanija informatsionno-kommunikatsionnych technologij”, Pressmeddelande 985–22–05–2023, 22 maj 2023.

54 Brics+ omfattar de ursprungliga Brics-länderna plus de som trätt in i Brics efter 2024, dvs. Egypten, Etiopien, Iran och Förenade Arabemiraten (Saudiarabiens anslutning är fortsatt oklar).

upp på dagordningen – varken vid något ministermöte eller i arbetsgruppen för IKT-frågor. Däremot vittnar det om en stark rysk strävan att använda Brics för att gynna sin egen digitala utveckling och politiska linje på området. Problemet för Ryssland är att dess egen befolkning och digitala marknad är för små. Det är Kina som kan erbjuda det som krävs vad gäller investeringar och digital teknologi samt tillsammans med Indien säkerställa att ett eventuellt BricsNet (eller BRIKSternet) alls kan bli livskraftigt.[55]

Som ordförandeland 2024 fortsatte Ryssland att driva på för att öka samarbetet på det digitala området, men frågan har inte varit högst prioriterat bland de övergripande målen.[56] I april höll expertarbetsgruppen sitt tionde möte i Moskva. Överlag dominerar allmänna skrivningar som minner om tidigare formuleringar i pressmeddelandet efter mötet. Ett konkret resultat var dock att länderna var överens om att upprätta en förteckning över ”kontaktpunkter” inom samtliga länder inom Brics+. Dessa kontaktpunkter skulle utgöra ett sätt att utbyta information om it-attacker och incidenter.[57] I november 2024 anordnade Ryssland en tävling för hackare inom ramen för Brics, en CTF (*Capture-the-flag*) där målet är att hitta så kallade flaggor, t.ex. hitta sårbarheter i program. Ryska hackerlag tog första och tredjeplatsen och antalet deltagande lag var ojämförligt störst från Ryssland. Syftet var enligt Ryssland att stimulera arbetet med att hitta och utbilda personal för cybersäkerhet i enlighet med Bricsländernas prioriterade mål.[58]

## Ett internationellt FN-avtal

Ryssland lade fram sitt första förslag till resolution om informationssäkerhet i FN redan 1998. Det ledde till att en dialog startades inom ramen för FN:s Group of Governmental Experts, som bestod av 25 utvalda länder. Redan tidigt stod det klart att västliga länders syn på hur informationssäkerhet bäst skulle garanteras internationellt var diametralt motsatt den som Ryssland drev på en rad nyckelområden. Frustrerad med bristen på framgång fortsatte Ryssland att övertala länder bilateralt samt inom organisationer som SCO och senare Brics att stödja den ryska linjen inom FN. Som ett led i detta lyckades också Ryssland skapa ett konkurrerande format inom FN för dessa diskussioner 2018, en Open-ended Working Group, i vilken alla FN-länder som så önskar kan delta.

Mot varandra står två olika synsätt på hur informationssäkerhet bör regleras internationellt. Västländerna anser att reglering och hantering av protokoll och funktioner bäst hanteras liksom tidigare med olika intressenter (*stakeholders*) involverade, flerpartsstyrning med alltifrån regeringar till icke-vinstdrivande organisationer som t.ex. driver ICANN och hanterar internets adressystem, domännamnssystemet. Ryssland, tillsammans med Kina anser att regeringar ska sluta avtal om internetreglering. Ytterligare en skillnad mellan västs och Rysslands ståndpunkt består i att väst fokuserar på att säkerställa funktionalitet medan Ryssland vill att regeringar ska rätt att styra vilken information som får spridas inom sina respektive länder.[59] För Ryssland har politisk kontroll över den egna befolkningen alltid varit ett prioriterat mål.[60]

Ryssland har konsekvent försökt att använda Brics för att etablera stöd för sin syn på internationell informationssäkerhet inom FN.[61] Enligt två ryska analytiker hade ”digital suveränitet” och samarbete för att nå ett internationellt bindande avtal på informationssäkerhetsområdet starkt stöd inom Brics:

> I vid bemärkelse kan digital suveränitet definieras som statlig självständighet inom digitala sfären och förmågan att självständigt realisera informationspolitik inom landet och på internationella arenan.[62]

Författarna reflekterar inte över hur en stats suveränitet kan kränkas av att en annan stat ”realiserar” sin politik på den internationella arenan. Enligt dem kan detta tillstånd av ”digital suveränitet” för samtliga stater helt enkelt förverkligas genom ett internationellt avtal.

55 Grigorij Bakunov i ”Totjka”, The Breakfast Show, 15 december 2024, YouTube (10:02 in i programmet).

56 Jekaterina Korostovtseva, ”Jurij Usjakov: BRIKS na dele vyrazjajet interesy mirovogo bolsjinstva”, *TASS*, 5 mars 2024.

57 Ryska UD, ”O 10-m zasedanii Rabotjej gruppy BRIKS po voprosam bezopasnosti v sfere ispolzovanija informatsionno-kommunikatsionnych technologij”, Pressmeddelande 710–17–04–2024, 17 april 2024.

58 Jelena Tjernenko, ”Rossija provela krupnyj turnir po kiberbezopasnosti s utjastijem stran BRIKS”, *Kommersant*, 17 november 2024.

59 Oleg Demidov, *Globalnoje upravlenije Internetom i bezopasnost v sfere ispolzovanija IKT* (Moskva: PIR-PRESS, 2016); Julien Nocetti, ”Contest and conquest”, *International Affairs*, vol. 91, nr. 1 (januari 2015), 111–30. Se även Carolina Vendil Pallin och Mattias Hjelm, ”Moscow’s Digital Offensive – Building Sovereignty in Cyberspace”, FOI Memo 7521, april 2021.

60 Dana Polatin-Reuben och Joss Wright, ”An Internet with BRICS Characteristics”, 4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14), San Diego, CA, 7 juli 2014, 4.

61 Alexander Ignatov. ”The BRICS Agenda on Internet Governance”, *International Organisations Research Journal*, vol. 17, nr. 2 (2022), 86–109.

62 Ignatov och Zinoveva, ”’Tsifrovoj suverenitet’ v povestke obedinenija BRIKS” [kapitelförfattarens översättning].

De hänvisar till att Bricsländerna har stött Rysslands förslag till FN-konventioner om internationell informationssäkerhet, respektive motverkande kriminell verksamhet på it-området (även om de också noterar att Brasilien stöder Europarådets konkurrerande Budapestkonvention om it-relaterad brottslighet).[63]

Av de initiativ på cyberområdet som Ryssland har drivit inom Brics är det samarbetet inom FN som kanske varit både främst prioriterat och mest framgångsrikt. Bricsländerna ställde sig positiva till Rysslands förslag till resolution mot cyberkriminalitet trots att den vaga formuleringen i resolutionen kan tas som intäkt för auktoritär övervakning på internet och trots att den underminerar existerande Budapestkonvention.[64] Ett internationellt avtal var också fortsatt ett prioriterat område i programförklaringen inför det ryska ordförandeskapet i Brics 2024.[65]

## 4.5 Slutsatser

Ryssland tog initiativet till att Brics alls blev en organisation och har dessutom varit pådrivande vad gäller samarbete på cyberområdet. Inte minst har Ryssland velat använda sig av Brics som plattform för att få igenom ett internationellt bindande avtal om informationssäkerhet inom FN och har nått vissa framgångar i det spåret. Ryssland har också föreslagit olika samarbetsformat på det digitala området, men har varit föga framgångsrikt vad gäller att få till stånd praktiska resultat. Ofta har det hela stannat vid generella uttalanden som inte binder Bricsländerna vid något konkret.

För Ryssland är också dilemmat att man har så pass lite att erbjuda på IKT-området jämfört med Kina och kanske även i viss mån Indien. Så var fallet redan före 2022, men dilemmat Ryssland befinner sig i har blivit alltmer tydligt efter att kriget mot Ukraina inleddes. Moskva behöver visa både för omvärlden och för opinionen på hemmaplan att landet inte står isolerat. Men samtidigt har Ryssland mindre än någonsin att erbjuda i termer av internationell prestige och lukrativa investeringar. På IKT-området torde länderna inom Brics+ snarare ha kommit till Moskva under ryska ordförandeskapet i hopp om att säkra investeringar, samarbeten och kontrakt med Kina snarare än med Ryssland. Att Ryssland skulle kunna övertala Bricsländerna till att bilda ett ”Bricsinternet” framstår utifrån dessa omständigheter som föga troligt.

63 Ignatov och Zinoveva, ”’Tsifrovoj suverenitet’ v povestke obedinenija BRIKS”.

64 United Nations Digital Library, Countering the use of information and communications technologies for criminal purposes: resolution, adopted by the General Assembly, 17 december 2018.

65 Karl Tichaze. ”Problematika mezjdunarodnoj informatsionnoj bezopasnosti v povestke BRIKS”, *Mezjdunarodnaja zjisn, Rossijskoje predsedatelstvo v BRIKS – 2024: Ukreplenije mnogostoronnosti dlja spravedlivogo globalnogo razvitija i bezopasnosti – Spetsialnyj vypusk*, Ryska utrikesministeriet, Moskva, 2024, 102–105.

# Referenser

Adindex. ”Bolsjinstvo rossijan ispolzujut VPN dlja dostupa k sotssetami i SMI” [Majoriteten av ryssarna använder VPN för att nå sociala medier och massmedia], 6 december 2023, hämtat 26 augusti 2025, *https://adindex.ru/news/researches/2023/12/6/317755.phtml*.

Babajev, Kirill, Andrej Kortunov m.fl. *Rossijsko-kitajskij dialog: model 2023*, RIAC, rapport nr. 87, Moskva: RIAC, 2023, hämtat 22 november 2024, *https://russiancouncil.ru/papers/Russia-China-2023-Report87.pdf*.

Bojko, Sergej. ”Problematiska mezjdunarodnoj informatsionnoj bezopasnosti na prosjtjadjach SjOS b BRIKS”. *Mezjdunarodnaja zjizn*, nr. 1 (2019), hämtat 11 november 2024, *https://interaffairs.ru/jauthor/material/2131*.

CNews. ”Roskomnadzor polutjit milliardov, tjtoby usilit blokirovki zapresjennych sajtov” [Roskomnadzor får miljarder för att stärka blockeringen av förbjudna sajter], 16 september 2024, hämtat 11 februari 2025, *https://www.cnews.ru/news/top/2024–09–10_vlasti_vydelyat_pochti_60_milliardov*.

ComNews. ”IKT dlja BRIKS: ot strategii k planu dejstvij”, 13 juli 2015, hämtat 12 september 2024, *https://www.comnews.ru/content/96465*.

Computer Swedens it-ordlista, *https://it-ord.computersweden.se/ord/*.

Demidov, Oleg. *Globalnoe upravlenie Internetom i bezopasnost v sfere ispolzovaniia IKT*. [Internationell reglering av internet och säkerhet i sfären av IKT-användning], Moskva: PIR-PRESS, 2016.

Dergacheva, Daria. ”The limits of compromise: how Yandex is falling apart”, *Russia.Post*, 23 juni 2022, hämtat 27 november 2024, *https://russiapost.info/society/the_limits_of_compromise_how_yandex_is_falling_apart*.

Elzes, Ksenia. ”Everything you need to know about Max, Russia’s state-backed answer to Whatsapp”, *The Moscow Times*, 28 August 2025, hämtat 10 oktober 2025, *https://www.themoscowtimes.com/2025/08/28/everything-you-need-to-know-about-max-russias-state-backed-answer-to-whatsapp-a90356*.

Engvall, Johan, Pär Gustafsson och Carolina Vendil Pallin. *Framtid med förhinder- Rysk teknisk FoU till 2030*, FOI-R--5204--SE, Stockholm: FOI, oktober 2021.

FOM. ”Novostnaja informatsija i televidenije” [Nyheter och tv], hämtat 21 augusti 2024, *https://fom.ru/SMI-i-internet/14984*.

Freedom House. ”Freedom on the Net – 2024: Russia”, Washington, DC: Freedom House, 2024, hämtat 13 november 2024, *https://freedomhouse.org/country/russia/freedom-net/2024*.

Försvarsministeriet. ”Kontseptualnyje vzgljady na dejatelnost vooruzjennych sil Rossjiskoj Federatsii v informatsionnom postranstve” [Konceptuell syn på Ryska Federationens Väpnade styrkors verksamhet inom informationssfären], hämtad 19 januari 2018, *http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle.*

”Grunderna för Ryska Federationens statliga politik inom informationssäkerhetsdomänen till 2020” (på ryska), antagen genom presidentorder nr. 1753, 24 juli 2013, hämtad 9 februari 2017, *http://www.scrf.gov.ru/security/information/document114/*.

Ignatov, Alexander.”The Digital Economy of BRICS: Prospects for Multilateral Cooperation”. *International Organisations Research Journal*, vol. 15, nr. 1 (2020): 31–62, hämtad 22 juli 2024, *https://iorj.hse.ru/data/2020/09/01/1577151228/%D0%92%D0%B5%D1%81%D1%82%D0%BD%D0%B8%D0%BA_2020_01_%D0%B0%D0%BD%D0%B3%D0%BB____final-22–46.pdf*.

Ignatov, Alexander. ”The BRICS Agenda on Internet Governance”. *International Organisations Research Journal*, vol. 17, nr. 2 (2022): 86–109, hämtad 22 juli 2024, *https://iorj.hse.ru/data/2022/08/03/1618070871/1Ignatov.pdf*.

Ignatov, Alexander och Jelena Zinoveva. ”’Tsifrovoj suverenitet’ v povestke obedinenija BRIKS”. RIAC, 24 januari 2024, hämtad 22 juli 2024, *https://iorj.hse.ru/data/2022/08/03/1618070871/1Ignatov.pdf*.

Internet Society – Pulse. ”IXP Tracker – Russia”, hämtat 9 februari 2025, *https://pulse.internetsociety.org/en/ixp-tracker/?country_code=RU&page=1*.

Kluge, Janis. *Russia's Transition to 5G: Stuck in a Regulatory Tug of War*. Report. Philadelphia: Foreign Policy Research Institute (FPRI), 20 August 2020. *https://www.fpri.org/article/2020/08/russias-transition-to-5g-stuck-in-a-regulatory-tug-of-war/*.

Kluge, Janis. ”The future has to wait: 5G in Russia and the lack of elite consensus”. *Post-Soviet Affairs*, vol. 37, nr 5 (2021): 489–505.

”Kontseptsija utjastija Rossijskoj Federatsii v obedinenii BRIKS” [Koncept för Ryska federationens deltagande i organisationen Brics], antagen av Rysslands president, 21 mars 2013, hämtad 13 november 2024, *http://kremlin.ru/events/president/news/17715*.

Korolev, Pavel. ”’Poljarnyj ekspress’ vstal na pauzu” [Polarexpressen har pausats], *ComNews*, 14 mars 2025, hämtat 5 februari 2026, *https://www.comnews.ru/content/238257/2025–03–14/2025-w11/1007/polyarnyy-ekspress-vstal-pauzu*.

Korostovtseva, Jekaterina. ”Jurij Usjakov: BRIKS na dele vyrazjajet interesy mirovogo bolsjinstva” [Jurij Usjakov: Brics utrycker i handling världsmajoritetens intressen], *TASS*, 5 mars 2024, hämtat 22 juli 2024, https//tass.ru/interviews/20149675.

Kortunov, Andrej. ”’Manifest novogo mirovogo porjadka’: razbirajem Kazanskuju deklaratsiju BRIKS” [”Manifest för en ny världsordning: Vi reder ut Brics Kazandeklaration]. RIAC, 25 oktober 2024, hämtat 7 november 2024, *https://russiancouncil.ru/analytics-and-comments/comments/manifest-novogo-mirovogo-poryadka-razbiraem-kazanskuyu-deklaratsiyu-briks/*.

Kreml. ”Obrasjtjenije Vladimira Putina v svjazi s natjalom predsedatelstva Rossii v BRIKS” [Vladimir Putins anförande i samband med inledningen av Rysslands ordförandeskap I BRICS], 1 januari 2024, hämtat 22 juli 2024, *kremlin.ru/events/president/news/73202*.

Lazanyuk, I och Revinova, S. ”Digital Economy in the BRICS countries: Myth or reality?”. Proceedings of the International Scientific and Practical Conference on Digital Economy, ISCDE, 2019, hämtat 22 juli 2024, *https://www.atlantis-press.com/article/125924651.pdf*.

Levadacentrum. ”Auditorija polzovatelej internet, sotsialnych setej, messendzjerov i VPN-servisov” [Interentanvändarauditorium, sociala medier, meddelandetjänster och VPN-tjänster], 23 april 2024, hämtat 22 juli 2024, *https://www.levada.ru/2024/04/23/auditoriya-polzovatelej-interneta-sotsialnyh-setej-messendzherov-i-vpn-servisov/*.

Levadacentrum. ”Kanaly polutjenija informatsii, sotsialnyje seti i messendzjery: posledstvija blokirovok” [Informationskanaler, sociala medier och meddelandetjänster: följder av blockeringarna], 11 oktober 2024, hämtat 11 februari 2025, *https://www.levada.ru/2024/10/11/kanaly-polucheniya-informatsii-sotsialnye-seti-i-messendzhery-posledstviya-blokirovok/*.

Mamikonjan, Olga. ”Kolitjestvo polzovatelej VPN v Rossii vyroslo potjti na 40 % v 2023 godu” [Antalet VPN-användare i Ryssland ökade med nästan 40 % under 2023], *Forbes*, 6 december 2023, hämtat 21 oktober 2024, *https://www.forbes.ru/tekhnologii/501873-kolicestvo-pol-zovatelej-vpn-v-rossii-vyroslo-pocti-na-40-v-2023-godu.*

Nadibaidze, Anna, ”Russia's Drive for AI: Do Deeds Match the Words?”, *The Washington Quarterly*, vol. 47, nr. 4 (2024): 137–54.

Niskanen, Juho. *Russia's ICT-infrastructure and Its Development Prospects in the Near Future*. Tammerfors: Finnish Defence Research Agency, 2023.

Nocetti, Julien. ”Contest and conquest: Russia and global internet governance”, *International Affairs*, vol. 91, nr. 1 (januari 2015): 111–30, *https://doi.org/10.1111/1468–2346.12189*.

”O razvitii iskusstvennogo intellekta v Rossijskom Federatsii” [Nationell strategi för utvecklingen av AI, presidentdekret nr. 490, 10 oktober 2019, hämtad 24 maj 2021, *http://static.kremlin.ru/media/events/files/ru/AH4x6HgKWANwVtMOfPDhcbRpvd1HCCsv.pdf*.

”Osnovy gosudarstvennoj politiki Rossiskoj Federatsii v oblasti mezjdunarodnoj informatsionnoj bezopasnosti na period do 2020 goda” [Grunder för Ryska Federationens politik inom området internationell informationssäkerhet till 2020], presidentorder nr. 1753, 24 juli 2013, hämtad 9 februari 2017, *http://www.scrf.gov.ru/security/information/document114/*.

Phokeer, Amreesh. ”How Isolated is the Russian Internet? Consequences of the war in Ukraine”, *Pulse*, 7 juni 2024, *https://pulse.internetsociety.org/blog/how-isolated-is-the-russian-internet-consequences-of-the-war-in-ukraine*.

Polatin-Reuben, Dana och Joss Wright. ”An Internet with BRICS Characteristics”, *4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14)*, San Diego, CA, 7 juli 2014, *https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf*.

Presidentdekret nr. 124, 15 februari 2024, hämtat 3 november 2025 *http://kremlin.ru/acts/bank/50326/page/1*.

Raymond, Mark och Justin Sherman. ”Authoritarian multilateralism in the global cyber regime complex”, *Contemporary Security Policy*, vol. 45, nr. 1 (2023): 110–40

Roberts, Cynthia. ”Polity Forum: Challengers or Stakeholders? BRICs and the Liberal World Order”, *Polity*, vol. 42, nr. 1 (januari 2010): 1–13, hämtat 21 augusti 2024, *https://www.journals.uchicago.edu/doi/full/10.1057/pol.2009.20*.

Roberts, Cynthia. ”Russia’s BRICs Diplomacy: Rising Outsider with Dreams of an Insider”. *Polity*, vol. 42, nr. 1 (januari 2010): 37–73, hämtat på WaybackMachine 22 juli 2024, *https://web.archive.org/web/20190307024220/http://pdfs.semanticscholar.org/f1cb/49f8c3423961ad7311128565deb74afde571.pdf*.

Ryska regeringen, ”Strategija razvitija otrasli svjazi Rossijskoj Federatsii na period do 2035 goda” [Strategi för att utveckla Ryska Federationens kommunikationsindustrin till 2035]. Regeringsorder nr. 3339-r, 24 november 2023, hämtat 8 januari 2025, *http://static.government.ru/media/files/Pc7fHuejbNvqv17b0RJNv0RIqTo20lUV.pdf*.

Ryska UD, ”Ob itogach zasedanija Rabotjej gruppy ekspertov gosudarstv-utjastnikov BRIKS po voprosam bezopasnosti v sfere ispolzovanija informatsionno-kommunikatsionnych technologij” [Om resultatet av Bricsländernas Ekspertarbetsgrupps möte för frågor inom sfären användande av informations och kommunikationsteknologi]. Pressmeddelande nr. 1229–19–06–2015, 19 juni 2015, hämtat 21 november 2024, *https://mid.ru/ru/foreign_policy/briks/1510609/*.

Ryska UD. ”Ob itogach 6-go zasedanija Rabotjej gruppy BRIKS po voprosam bezopasnosti v sfere ispolzovanija informatsionno-kommunikatsionnych technologij” [Om resultatet av Brics Arbetsgrupps 6:e möte för frågor inom sfären användande av informations och kommunikationsteknologi]. Pressmeddelande nr. 1301–28–08–2020, 28 augusti 2020, hämtat 21 november 2024, *https://mid.ru/ru/foreign_policy/briks/1440635/*

Ryska UD. ”O 9-m zasedanii Rabotjej gruppy BRIKS po voprosam bezopasnosti v sfere ispolzovanija informatsionno-kommunikatsionnych technologij” [Om 9:e mötet för Brics arbetsgrupp för frågor inom sfären användande av informations- och kommunikationsteknologier], Pressmeddelande 985–22–05–2023, 22 maj 2023, hämtat 12 september 2024, *https://mid.ru/ru/foreign_policy/briks/1871756/*.

Ryska UD. ”O 10-m zasedanii Rabotjej gruppy BRIKS po voprosam bezopasnosti v sfere ispolzovanija informatsionno-kommunikatsionnych technologij” [Om 10:e mötet för Brics arbetsgrupp för frågor inom sfären användande av informations- och kommunikationsteknologier], Pressmeddelande 710–17–04–2024, 17 april 2024, hämtat 28 november 2024, *https://mid.ru/ru/foreign_policy/briks/1944857/*.

Rysslands informationssäkerhetsdoktrin, presidentdekret nr. 646, 5 december 2016, hämtad 11 augusti 2017, *http://static.kremlin.ru/media/acts/files/0001201612060002.pdf*.

Rysslands nationella säkerhetsstrategi till 2020, presidentdekret nr. 537, 12 maj 2009, hämtad 15 november 2024, *https://www.garant.ru/products/ipo/prime/doc/95521/*.

Rysslands nationella säkerhetsstrategi, presidentdekret nr. 683, 31 december 2015, hämtad 26 september 2017, *http://www.scrf.gov.ru/security/docs/document133/*.

Rysslands nationella säkerhetsstrategi, presidentdekret nr. 400, 2 juli 2021, hämtad 15 november 2024, *http://scrf.gov.ru/media/files/file/l4wGRPqJvETSkUTYmhepzRochb1j1jqh.pdf*.

Rysslands utrikespolitiska koncept, presidentdekret nr. 229, 31 mars 2023, *http://scrf.gov.ru/media/files/file/vugNZ0pvJNFgKhkD6psAwhp8jAi8p2Qt.pdf*.

Sergunin. A. A. ”Russia’s Strategies towards BRICS: Problems and Opportunities”, *Vestnik RUDN. International Relations*, vol. 20, nr. 3 (2020): 534–42, *https://doi.org/10.22363/2313–0660–2020–20–3-534–542*.

Šćepanović, Janko. ”The 2024 BRICS Summit in Kazan: Another Russian Attempt to Regain Diplomatic Status”. PONARS Eurasia Policy Memo, nr. 917, november 2024, *https://www-ponarseurasia-org.b-cdn.net/wp-content/uploads/2024/10/PEPM_S%CC%8Cc%CC%81epanovic%CC%81_Nov2024_final.pdf*.

Sinkkonen, Elina och Jussi Lassila. ”Digital Autoritarianism and Technological Cooperation in Sino-Rusian Relations: Common Goals and Diverging Standpoints”. I *Russia-China Relations : Emerging Alliance or Eternal Rivals?,* red. Sarah Kirchberger, Svenja Sinjen och Nils Wörmer. Cham.: Springer, 2000, *https://doi.org/10.1007/978–3-030–97012–3_9*: 165–184.

Sizov, Ilja. ”’Roskosmos’ podelitsia tjastotami” [”Roskosmos” delar med sig av frekvenser], *Kommersant*, 28 oktober 2024. *https://www.kommersant.ru/doc/7265578*.

”Sovesjtjanije s tjlenami pravitelstva” [Sammanträde med medlemmar i regeringen], Kremls hemsida, 4 juni 2025, hämtat 10 oktober 2025, *http://www.kremlin.ru/events/president/news/77099*.

TeleGeography, ”Submarine Cable Map”, hämtat 11 februari 2025, *https://www.submarinecablemap.com/country/russia*.

Tichaze, Karl. ”Problematika mezjdunarodnoj informatsionnoj bezopasnosti v povestke BRIKS” [Internationella informationssäkerhetsproblematiken på BRICS agenda]. *Mezjdunarodnaja zjisn, Rossijskoje predsedatelstvo v BRIKS – 2024: Ukreplenije mnogostoronnosti dlja spravedlivogo globalnogo razvitija i bezopasnosti – Spetsialnyj vypusk* [*International Affairs*, Ryska ordförandeskapet för BRICS – 2024: Stärkandet av multilateralism för en rättvis global utveckling och säkerhet – specialutgåva], Moskva: Ryska UD, 2024: 102–105, hämtat 22 juli 2024, *https://brics-russia2024.content.rcmedia.ru/upload/docs/%D0%91%D0%A0%D0%98%D0%9A%D0%A1_2024.pdf*.

Tjernenko, Jelena. ”Rossija provela krupnyj turnir po kiberbezopasnosti s utjastijem stran BRIKS” [Ryssland genomförde en stor cybersäkerhetstävling med deltagare från Brics-länderna], *Kommersant*, 17 november 2024, *https://www.kommersant.ru/doc/7310233*.

United Nations Digital Library. Countering the use of information and communications technologies for criminal purposes: resolution, adopted by the General Assembly, 17 december 2018, hämtat 28 november 2024, *https://digitallibrary.un.org/record/1656199*.

Vendil Pallin, Carolina. ”Internet Control through ownership: the case of Russia”, *Post-Soviet Affairs*, vol. 33, nr. 1 (2017): 16–33.

Vendil Pallin, Carolina. *Nyckelaktörerna för rysk cyberstratetgi 2000–2020*, FOI-R--5025--SE, Stockholm: FOI, oktober 2020.

Vendil Pallin, Carolina. *Rysslands cyberberedskap på hemmaplan*, FOI-R--5611--SE, Stockholm: FOI, augusti 2024.

Vendil Pallin, Carolina och Mattias Hjelm. ”Moscow’s Digital Offensive – Building Sovereignty in Cyberspace’’, FOI Memo 7521, april 2021.

Yushenko, Michael. ”Internet governance in Russia: A brief history of the term and the process”, i William J. Drake (red.), *The working group on Internet governance: 10th Anniversary reflections*, APC, 2015: 117–21, *https://www.apc.org/sites/default/files/IG_10_Final_0.pdf*.

# 5. Indien – ”Ickevästlig men inte antivästlig”

*Samuel Neuman Bergenwall*

Indien använder Brics som ett verktyg för att främja sina ekonomiska och politiska intressen. Förutsättningarna för samarbete inom organisationen har skiftat över tid och påverkas i hög grad av Indiens bilaterala relationer till Kina respektive USA.

## 5.1 Indiens relation med Brics

Indien började utmejsla en tredje väg mellan öst och väst på 1950-talet genom att utveckla multilaterala samarbeten med Kina och andra stater i det som idag benämns som det globala syd. New Delhi var en drivande kraft bakom såväl Bandungkonferensen 1955, om afrikansk-asiatiskt samarbete, som den alliansfria rörelsen.[1] Men Kinas militära angrepp på Indien 1962, om omtvistade gränsområden kring Himalaya, åtföljdes av spända relationer i ett drygt kvartssekel.[2] Möjligheten till multilateralt samarbete inom det globala syd komplicerades ytterligare efter Indiens fördrag med Sovjetunionen 1971, som ledde till ett nära indiskt-sovjetiskt strategiskt samarbete under återstoden av det kalla kriget.

Efter Sovjetunionens sammanbrott justerade Indien sin säkerhetspolitiska kurs och anammade en så kallad *multi alignment*-strategi.[3] I linje med den knöt Indien närmare band till både västvärlden och det globala syd, samtidigt som man bibehöll goda förbindelser till Ryssland. Indien antog också en mer proaktiv hållning till multilateralt samarbete och blev medlem i en rad institutioner.[4] Vissa av dem leds av Kina och Ryssland, som samarbetsorganisationen Shanghai Cooperation Organization, och andra av asiatiska stater, som sammanslutningar inom The Association of Southeast Asian Nations. Indien medverkar också i institutioner där västerländska stater är tongivande, såsom Quadrilateral Security Dialogue (Quad).[5]

Det som framför allt möjliggjorde Indiens beslut att bli medlem i Brics var förbättrade relationer till Kina. Men övriga medlemmar hade Indien sedan tidigare goda relationer. Under 1990-talet kom Indien och Kina överens om att stabilisera situationen i gränsområdena mellan länderna och att inte låta territorialdispyten förhindra samarbete på andra områden. Kina blev därefter och på kort tid Indiens största handelspartner liksom samarbetspartner i multilaterala fora.[6]

Genom att bli medlem i Brics ämnade Indien primärt att få stöd för tre nationella intressen: att utveckla sin ekonomi genom handel och investeringar; att verka för en multipolär världsordning; och att stärka sin ställning internationellt. Indien uppfattar Brics delvis som ett instrument för öka sitt inflytande i globala institutioner, såsom Världsbanken, Internationella valutafonden (IMF), Världshandelsorganisationen och för att få en permanent plats i ett utökat säkerhetsråd i FN.[7] Över tid har Indien även använt Brics för att främja intressen som rör utbildning, hälsovård och infrastruktur, men har även bidragit till samarbeten på säkerhetsområdet, till exempel om kontraterror och informationsteknologi.[8] Indien vill dock inte att Brics ersätter Bretton Woods-institutionerna; under mötet i Kazan 2024 underströk premiärmister Narendra Modi att “vi måste vara noga med att garantera att denna organisation [Brics] inte uppfattas ersätta globala institutioner.”[9]

1 Den alliansfria rörelsen samlade under det kalla kriget länder i det som då kallades tredje världen. De ville undvika att ansluta sig till någon av de ideologiska blocken men samtidigt bevaka medlemsstaternas intressen i världspolitiken.

2 Alka Acharya, ”China”, i *The Oxford Handbook of Indian Foreign Policy,* red. David Malone et al., (Oxford: Oxford University Press, 2015), 356–60.

3 Rahul Mishra, ”From non-alignment to multi-alignment: assessing India’s foreign policy shift”, *The Round Table: The Commonwealth Journal of International Affairs*, vol. 112, nr. 1 (2023): 43–56. Ashley J. Tellis, ”Non-Allied Forever: India’s Grand Strategy According to Subrahmanyam Jaishankar”, *Carnegie*, 3 mars 2021.

4 Samir Saran, ”India’s Contemporary Plutilateralism” i Malone et al 2015), 623.

5 I Quad ingår, förutom Indien, länderna Australien, Japan och USA.

6 Acharya, ”China”, 362–68.

7 Saran, ”India’s Contemporary Plutilateralism”, 623–27.

8 Harsh V. Pant och Rajoli Siddharth Jayaprakash, ”In Kazan, the Global South makes a point about Brics”, *The Hindustan Times*, 24 oktober 2024.

9 Sudhi Ranjan Sen, ”Modi Says BRICS Must Avoid Being an Anti-West Group as It Grows”, *Bloomberg*, 24 oktober 2024.

Djupare strategiskt samarbete inom Brics försvåras i dag av att Indiens relationer till Kina har blivit sämre samtidigt som samarbetet med USA har fördjupats. Under 10-talet försvagades gradvis Indiens relationer till Kina och 2020 ägde en militär sammandrabbning rum längs de omtvistade gränsområdena med dödsoffer på bägge sidor. De indisk-kinesiska intressekonflikterna har i sin tur spillt över på Brics-samarbetet. Forskaren Harsh Pant beskriver situationen träffande:

> Det fanns en tid när New Delhi och Peking till och med kunna tala med en röst om globala utmaningar. Men i dag håller skiljelinjerna inom Brics på att bli skarpare. /…/ Ryssland och Kina försöker svänga om grupperingens geoekonomiska inriktning till en öppen geopolitisk sådan och [göra Brics] till en anti-västlig plattform, fastän Indiens och Kinas representanter är allt mer obekväma med att sitta i samma rum.[10]

Parallellt med att Kina och Ryssland under det senaste decenniet har rört sig i alltmer anti-västlig riktning har Indien i flera avseenden gått åt motsatt håll. USA har blivit Indiens viktigaste säkerhets- och försvarspolitiska partner, och de indiska relationerna till Västeuropa har utvecklats positivt.[11] Utrikesminister Subrahmanyam Jaishankar tydliggjorde Indiens position visavis väst vid säkerhetskonferensen i München 2024:

> Jag tror det är viktigt att idag göra en distinktion mellan att vara icke-västlig och anti-västlig. Jag skulle inte enbart karakterisera Indien som ett land som inte är icke-västligt, utan också som [ett land som] har extremt starka relationer med västliga stater.[12]

Jaishankar menar vidare att multilaterala institutioner, som Brics och Quad, tjänar skilda indiska syften.[13] Det innebär i sin tur begränsningar för hur djupt Indiens samarbete kan sträcka sig inom enskilda sammanslutningar. För Indien är således Brics ett av flera multilaterala redskap för att uppnå specifika och avgränsade nationella mål, men potentiellt också "en strategisk tillgång som ger djup till [Indiens] utrikespolitik utan att hindra utvecklingen av säkerhetsförbindelser med USA."[14]

## 5.2 Internets utveckling i Indien

Internets fysiska utveckling i Indien skedde initialt långsamt och berörde främst myndigheter, forskningsinstitutioner och mjukvaruexportörer. I slutet av 1980-talet upprättades ett indiskt nätverk för forskare genom stöd från FN.[15] Indien byggde också ut ett inomstatligt nätverk för bland annat departement, myndigheter och styrande på delstatsnivå.[16] I början av 1990-talet etablerades dessutom ett ytterligare nätverk för industriparker med syftet att främja mjukvaruexport.[17] Det statliga telekombolaget Videsh Sanchar Nigam ansvarade för alla tre näten, men också för att ge allmänheten uppkoppling mot internet, något som skedde i maklig takt.[18]

Vad gäller det *fysiska lagret* (se kapitel 2) har utbyggnaden av internetinfrastrukturen accelererat under de senaste tio–femton åren genom ett indiskt politiskt fokus på digitalisering och genom ett ökat deltagande av privata företag. Sedan Bharatiya Janata Party (BJP, indiska folkpartiet) kom till makten 2014 har regeringar under ledning av premiärminister Narendra Modi prioriterat digitalisering av staten, samhället och ekonomin. BJP har som mål att hela den indiska befolkningen ska få tillgång till uppkoppling med bredband. För att uppnå detta har BJP låtit den privata sektorn, framför allt konglomeratet Reliance Industries, ta över mycket av utbyggnaden av internet, något som i sin tur haft positiv effekt. Sedan 2022 har frekvensspektrum auktionerats ut till de privata bolagen Reliance Jio, Bharti Airtel, Vodafone Idea och Adani Data Networks för utbyggnad av femte generationens (5G) internet.[19] Mellan 2014 och 2024 ökade antalet abonnenter med

10 Harsh V. Pant, red., "From BRICS to BRICS Plus: Old Partners and New Stakeholders", *ORF Special Report No. 214*, Observer Research Foundation, september 2023.

11 Samuel Neuman Bergenwall, *Indien som säkerhetspolitisk aktör: konsekvenser för svenska försvarsrelationer*, FOI-R--5588--SE, (Stockholm: FOI, 2024).

12 ANI, "'Clearly, 30 countries saw value in it...': Jaishankar commends BRICS at Munich Security Conference", 17 februari 2024.

13 Observer Research Foundation, "To Us, They Serve Different Purposes: EAM Jaishankar on India's BRICS & QUAD Diplomacy", *YouTube*, 7 november 2024.

14 Jagannath Panda, "India's BRICS Balancing Act", United States Institute for Peace, 17 oktober 2024.

15 Grey E. Burkhart et al, "The Internet in India: Better Times Ahead?", *Communications of the ACM*, vol. 41, nr. 11 (1998): 21–26.

16 National Informatics Centre, Government of India, "NICNET".

17 Ministry of Electronics & Information Technology, "Software Technology Parks of India (STPI)" .

18 Grey E. Burkhart et al, "The Internet in India", 21–26.

19 Department of Telecommunications, Ministry of Communications, Government of India, "Auction_2022_Bid_Ranking", 5 september 2022. Department of Telecommunications, Ministry of Communications, Government of India, "Auction_2024_Bid_Ranking", 17 september 2024.

bredbandsuppkoppling från 250 till 950 miljoner.[20] Även om majoriteten av dessa fortfarande är stadsbor hade ca 95 procent av Indiens byar täckning för mobilt bredband 2024.[21] Uppkopplingen mot internet skedde till 96 procent via trådlöst internet och 4 procent med kabelanslutning.[22]

Indien har även i snabb takt ökat sin kapacitet för datalagring, som idag är näst störst i Asien efter Kina. Indien har fem större statliga datacenter, majoriteten i de södra delarna av landet.[23] Privata företag står för omkring 85 procent av kapaciteten och de satsar nu stort på att öka förmågan till datalagring ytterligare. Indiens datalagringskapacitet bedöms mer än fördubblas mellan 2024 och slutet av 2027.[24] Indiens internetknutpunkter (IXP:er) har också blivit fler och uppgår i dag till 34 stycken.[25] 2023 antog Indien en ny lagstiftning, The Telecommunications Act. Sedan dess har statliga Telecom Regulatory Authority of India bett att få ta del av perspektiv på hur IXP:erna ska regleras framgent, bland annat från privata aktörer.[26] Det pågår därför en debatt i Indien om hur den nya lagstiftningen borde implementeras och dess innebörd för IXP:er.[27]

Utbyggnaden av undervattenskablar till och från Indien har också skett i snabb takt. Indiens internet är i dag länkat till omvärlden via omkring 20 internationella fiberoptiska undervattenskablar. De når det indiska fastlandet genom minst 14 stationer i fem städer, de flesta i Mumbai och Chennai. Mottagarstationer finns även i de sydindiska städerna Cochin, Thoothukudi och Trivandrum. De flesta av de undervattenskablar som anlöper Indien ägs av de privata indiska företagen Reliance Jio, Tata Communications och Bharti Airtel, ofta i konsortier tillsammans med utländska bolag. Det statliga indiska telekombolaget Bharat Sanchar Nigam Ltd. (BSNL) spelar en mindre roll, som ägare av nya undervattenskablar till Sri Lanka och till de strategiskt viktiga ögrupperna Andamanerna, Nicobarerna och Lakshadweep.[28]

Några av undervattenskablarna saknar dock helt indiskt ägarskap. Brittiska 3i Infrastructure äger två äldre undervattenskablar via bolaget Global Cloud Xchange.[29] Tre nya kablar – Raman, Mist och 2Africa – har också utländska ägare. Raman binder samman Indien med Sydostasien och ägs av ett bolag med kopplingar till Japan. Mist knyter samman Indien med arabstater i Röda havet och Persiska viken och ägs av ett konsortium bestående av amerikanska Google, italienska Sparkle och omanska Omantel. 2Africa ägs i sin tur av ett konsortium bestående av bland andra amerikanska Meta och Chinese Mobile.[30] De indiska privata företagen är till synes benägna att samarbeta med utländska bolag, oavsett ursprung. Trots de politiska konflikterna med Kina, spelar kinesiska företag idag en viktig och växande roll. Två nya kablar, India Asia Xpress och India Europe Xpress, ägs gemensamt av Reliance Jio och Chinese Mobile, bedömdes bli operativa under 2025 och kraftigt öka Indiens bandbredd.[31] Sammantaget återspeglar Indiens samarbeten på havsbotten dess övergripande *multi alignment*-strategi.

För utbyggnaden av sina mobila nätverk har Indien vänt sig till utländska företag, framför allt Huawei, ZTE, Samsung, Ericsson och Nokia. Indien ålägger företagen att samarbeta med indiska partners, såsom Reliance Jio, Bharti Airtel och Vodafone Idea och BSNL. Alla dessa fyra indiska telekombolag uppges ha kinesisk teknologi i sina 3G- och 4G-nätverk.[32] För utbyggnaden av 5G-nätverken har dock Indien vänt Kina ryggen. I maj 2021, ett knappt år efter den kinesisk-indiska militära konfrontationen, meddelades det att indiska företag kunde inleda samarbeten om 5G med tre företag:

20 Telecom Regulatory Authority of India, ”The Indian Telecom Services: Yearly Performance Indicators 2023–2024”, 14 augusti 2024.
21 Press Information Bureau, Government of India, ”Universal connectivity and Digital India initiatives reaching to all areas, including tier-2/3 cities and villages”, 2 augusti 2024.
22 Telecom Regulatory Authority of India, ”The Indian Telecom Services: Yearly Performance Indicators 2023–2024”, 14 augusti 2024.
23 Software Technology Parks of India, Ministry of Electronics & Information Technology, Government of India, ”Data Center: STPI’s Tier-III Data Centers”.
24 ICRA, ”India’s data centre operational capacity to double in next 30 months to 2,000–2,100 MW by FY2027”, 22 oktober 2024.
25 Internet Society Pulse, ”IXP Tracker: India”.
26 Telecom Regulatory Authority of India, ”Consultation Paper on The Terms and Conditions of Network Authorisations to be Granted Under the Telecommunications Act, 2023”, Consultation Paper No. 16/2024, 22 oktober 2024.
27 Kamya Pandey, ”Battle lines drawn for regulating Internet Exchange Points in India: Extreme and NIXI vs Vodafone Idea”, *Medianama*, 28 november 2024.
28 Submarine Cable Networks, ”India”. Submarine Cable Map, ”India”.
29 3i Infrastructure, ”Global Cloud Xchange”, hämtat 14 december.
30 Submarine Cable Map.
31 Times of India, ”Big Boost for India’s internet quality! Three large undersea cable projects to expand capacity by more than four times”, 21 augusti 2024.
32 Manuel Gonzalo et al, ”5G Kick-off in India and Brazil: InterState Competition, National Systems of Innovation, and Catch-up Implications for the Global South”, *Seoul Journal of Economics*, vol. 36 nr. 1 (2023), 64.

Samsung, Nokia och Ericsson. I och med att Huawei och ZTE inte nämndes uteslöt Indien i praktiken kinesiska företag från utbyggnaden av 5G-nät i landet. Mukesh Ambani, Asiens rikaste man och ordförande för Reliance Industries, har lovat att Reliance Jio, Indiens största mobiloperatör, inte kommer att använda en enda kinesisk komponent i sitt 5G-nätverk.[33] Reliance Jio har också kommit längst med utvecklingen av landets enda *standalone*-nätverk för 5G tillsammans med Ericsson. För samarbetet har Ericsson fått det största enskilda lånet i svenska Exportkreditnämndens historia.[34] Nokia har i sin tur skrivit under ett avtal med Indiens näst största mobiloperatör, Bharti Airtel, om utvecklingen av deras 5G-nät.[35] Mycket tyder således på att nordiska företag, och Samsung, kommer att dominera Indiens 5G-nät på bekostnad av kinesiska aktörer.

Marknaden för smarta telefoner i Indien har också exploderat och antalet sålda enheter uppskattas uppgå till cirka 650 miljoner.[36] Kina dominerar marknaden med märken som Vivo, Xiaomi, Realme och Oppo.[37] Tillverkare från Kina för också dialog med indiska bolag om gemensam tillverkning i Indien, men det uppges finnas betydande hinder mot faktiskt samarbete, till exempel genom att indiska myndigheter försöker begränsa Kinas dominans på marknaden. Indiens ekobrottsmyndighet, The Enforcement Directorate, utreder Vivo för misstankar om penningtvätt, samtidigt som den indiska regeringen anklagar Vivo, Oppo och Xiaomi för att ha undflytt tullar och skatter.[38] Kinesiska aktörer spelar en mindre roll på den indiska marknaden för persondatorer jämfört med den för smarta telefoner; marknaden för persondatorer delas mellan kinesiska, taiwanesiska, sydkoreanska och amerikanska företag.[39]

Indien har även tagit steg mot att öka satellituppkopplingen i landet, bland annat för att ge otillgängliga områden tillgång till internet. Hösten 2024 lanserade statliga BSNL en tjänst för uppkoppling via satellit i krissituationer.[40] Indiska departementet för telekommunikation står också i begrepp att allokera frekvensspektrum till privata aktörer, där amerikanska, europeiska och indiska företag, visat intresse.[41] I Indien pågick en debatt om landet ska betona kommersiell logik och låta amerikanska Starlink få en central roll på marknaden, eller istället prioritera principen om nationell suveränitet och ge en större plats åt Reliance Jio.[42] Efter Donald Trumps tillträde som president i USA 2025 har emellertid både Reliance Jio och Bharti Airtel skrivit under överenskommelser om samarbete med Starlink.[43] I juni 2025 tilldelades Starlink en licens för att kunna erbjuda sina satelittjänster i Indien.[44]

## 5.3 Internets samtida tillstånd i Indien

När det kommer till det *logiska lagret* (se kapitel 2) är amerikanska mjukvaror är kraftigt överrepresenterade i indiska smarta mobiltelefoner. Googles Android OS är det i särklass vanligaste operativsystemet; WhatsApp, Facebook, YouTube, Instagram är bland de mest använda applikationerna.[45] Kinas roll som mjukavaruleverantör till Indien har samtidigt avtagit. Några veckor efter den kinesisk-indiska militära sammandrabbningen 2020 förbjöds ca 60 kinesiska applikationer, bland andra TikTok och WeChat, som en följd av en rekommendation från Indiens inrikesministerium.[46] Sedan dess har ytterligare kinesiska applikationer svartlistats. Det har också lagts större fokus på att utveckla inhemska mjukvaror i Indien. The Indian Institute of Technology har exempelvis tagit fram ett operativsystem för smarta telefoner vid namn *BharOS*, som hittills inte fått något större genomslag. Men Dharmendra Pradhan, minister för utbildning, kompetensutveckling och entreprenörskap, menar att BharOS ”är ett viktigt initiativ i riktning mot att infria

33 IANS, ”Jio only one to not use Chinese components: Mukesh Ambani told Donald Trump”, *Mint*, 28 februari 2020.
34 EKN, ”Record deal behind record-time 5G rollout in India”, 7 november 2023, hämtat 14 december 2024.
35 Nokia, ”Nokia wins multi-billion 5G extension deal from Bharti Airtel for its India operations”, 20 november 2024
36 Telecomelead, ”India’s used smartphone market grows amid challenges in new device sales”, 16 oktober 2024.
37 IDC, ”Indian Smartphone Market Grew 7% YoY in 1H24, Reaching 69 Million Units”, 13 augusti 2024.
38 Vaddha Mukherjee, ”Chinese smartphone giants seek Indian partnerships amid govt push”, *Business Standard*, 4 juli 2024.
39 IDC, ”Indian PC Market Grew 7.1% YoY with 3.39 Million Units Shipped in 2Q2024, says IDC”, 19 augusti 2024.
40 *Times of India*, ”BSNL India’s first direct-to-direct-device satellite service: What it means for users, key features and more”, 15 november 2024.
41 Abhishek Chakraborty, Reuters, ”Starlink In India Soon? Elon Musk Takes On Mukesh Ambani’s Reliance Jio”, 12 november 2024.
42 Ehtesham Haque, ”Satellite internet showdown: Starlink vs Jio and what’s best for India’s future”, *The Times of India*, 16 oktober 2024.
43 Jocelyn Fernandes, ”After Airtel, Jio brings Elon Musk’s Starlink to customers in India. What’s on offer?”, *Mint*, 12 mars 2025.
44 Press Trust of India, ”Elon Musk’s Starlink gets licence to start India services amid feud with Trump”, *The Hindu*, 6 juni 2025.
45 Similarweb, ”Top Apps Ranking: India”.
46 Press Bureau of India, Ministry of Electronics & IT, ”Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order”, 29 juni 2020.

premiärminister Shri Narendra Modijis[47] vision om digital infrastruktur i Indien som är stark, inhemsk och oberoende.”[48] Det finns också ett antal populära indiska applikationer, såsom PhoneMe (för betalningar).

## Indisk it-tjänsteexport

En viktig aspekt av internetutvecklingen i Indien rör export av it-tjänster. Under de senaste 20 åren har indiska konsultbolag och mjukvaruutvecklare inte bara förvandlat sydindiska storstäder till globala it-hubbar, utan också bidragit till den högteknologiska utvecklingen i USA och Europa genom outsourcing och arbetskraftinvandring. Indiens it-tjänstehandel med västerländska nationer är i dag central för den indiska ekonomin. Den amerikanska investmentbanken Goldman Sachs beskriver Indien som världsledare i tjänsteexport, menar att den årliga ökningstakten länge varit dubbelt så hög som genomsnittet i världen och att förklaringen framför allt har att göra med it-tjänsterna. Goldman Sachs bedömer att den indiska tjänsteexporten 2030 kommer att vara värd ca 800 miljarder dollar.[49] Export av konsulttjänster av indiska it-jättar som Wipro, Infosys, HCL, och Tata Consultancy Services är viktig för Indiens ekonomi och diplomati.

Den indiska it-relaterade tjänsteexporten går främst till västliga och engelskspråkiga länder.[50] Av den indiska exporten går 62 procent till USA, 17 procent till Storbritannien och 11 procent till EU, enligt Indiens myndighet för elektronik och informationsteknologi. Genom it-tjänsteexporten har indiska medborgare blivit integrerade i västerländska företags interna digitala processer. Personer med indisk bakgrund utgör en stor andel av it-experterna i Silicon Valley. Många har dessutom avancerat till höga chefspositioner i amerikanska företag, såsom Satya Nadella, vd för Microsoft, Sundar Pichai, vd för Google och Alphabet, Arvind Krishna, vd för IBM, Shantanu Narayen, vd för Adobe, och Sanjay Mehrotra, vd för halvledartillverkaren Micron.[51] Storskalig immigration av indisk it-expertis är märkbar även i EU, till exempel i Sverige. Mellan 2013 och 2023 ökade antalet personer med indiskt ursprung i Sverige nästan 300 procent, från knappt 22 000 till över 58 000.[52] Invandringen sker bland annat med hjälp av indiska it-konsultbolag som erbjuder svenska företag it-expertis, till exempel när det gäller mjukvaruutveckling.

## Indisk lagstiftning och nationell suveränitet

Lagstiftningen i Indien påverkar också internets tillstånd i landet. Indisk lagsstiftning innebär i dagsläget inga större begränsningar av utflöde av nationellt genererade data. Samtidigt har indiska myndigheter stora befogenheter att på vaga grunder begränsa allmänhetens tillgång till information.

Indien lägger generellt stor vikt vid principen om nationell suveränitet och relaterade principer som territoriell integritet och ickeinblandning i andra staters interna angelägenheter. I praktiken skiljer sig graden av implementering av suveränitetsprincipen åt mellan olika områden.[53] Frågan om suveränitet på internet var högt upp på den indiska agendan mellan 2018 och 2023 då Indiens första lagstiftning om dataskydd bereddes. Tidiga utkast och lagförslag betonade vikten av att data hölls inom landet. Under processens gång urvattnades betoningen av nationell suveränitet. I den lag som i slutändan antogs, Digital Personal Data Protection Act (DPDPA) 2023, finns inga krav på begränsningar i fråga om transnationella dataflöden. Aktörer såsom den indiska centralbanken tillåts dock begränsa information inom landet.[54]

Forskarna Rudra Chaudhuri och Arjun Kang Joseph menar utifrån sin analys av DPDPA att Indien inte lägger så mycket fokus på suveränitetsprincipen som ibland hävdas och att staten inte bidrar mer än andra till ”balkaniseringen” av internet. De påstår att Indiens förhållningssätt drivs av ekonomiska och

47 En artig form av premiärminister Modis namn. För att visa aktning i Indien så kan man använda ”shri” (motsvarande ”herr”) före förnamnet och ”ji” som ett suffix till efternamnet.

48 Press Bureau of India, Ministry of Education, ”Shri Dharmendra Pradhan with Shri Ashwini Vaishnaw successfully tests the ‘BharOS’, a Made in India mobile operating system developed by IIT Madras”, 24 januari 2023.

49 Goldman Sachs, ”How India’s services economy became a world leader”, 13 januari 2024. Se även Världsbanken, ”Trade in services (% of GDP) – India” (1975–2024).

50 Press Trust of India, ”Software services export grows to $205.2 bn in FY24, US major destination”, *Business Standard*, 18 oktober 2024.

51 The Economic Times, ”21 Indian-origin CEOs of billion dollar companies”, 29 november 2023.

52 SCB, ”Befolkning, antal efter födelseland och år”, Statistikdatabasen.

53 Rudra Chaudhuri och Nabarun Roy, ”India and the sovereignty principle: the disaggregation imperative”, *India Review*, vol. 23, nr. 2 (2024): 89–94.

54 Rudra Chaudhuri och Arjun Kang Joseph, ”Living in a fragmented world: India’s data way”, *India Review*, vol. 23, nr. 2 (2024): 154–76.

säkerhetsrelaterade faktorer, inte av behovet av datakontroll.[55] Forskaren Anirudh Burman, som också analyserat dataskyddslagstiftningen, instämmer i att DPDPA inte begränsar gränsöverskridande dataflöden, men varnar för att fler indiska myndigheter kan följa centralbankens fotspår genom att själva införa nationella begränsningar av data. Han menar vidare att effekterna av DPDPA först kommer att visa sig om några år, i den faktiska implementeringen av lagstiftningen.[56]

Den november 2025 utfärdades regleringar baserade på den nya lagstiftningen. Regeringen menar att den stärker medborgarna och skyddar den privata integriteten, t.ex. genom att begränsa makten hos dataförvaltare, såsom utländska digitala plattformar.[57] Kritiken har dock varit hård från civilsamhället. Indiska tidningar och ickestatliga organisationer menar att regleringarna stärker statens makt på individernas bekostnad, utvattnar den lagstadgade rätten till information samt hotar pressfriheten.[58] I början av december utfärdade även ministeriet för kommunikation en föreskrift om att tillverkare av smarta telefoner måste installera en cybersäkerhetsapplikation, *Sanchar Saathi,* på alla indiska enheter inom 90 dagar. Kritiken inom civilsamhället och från tillverkare, som Apple, var massiv. Indiska officiella representanter menade därefter att det ska vara möjligt att radera applikationen.[59]

Andra lagar ger den indiska staten långtgående befogenheter till informationskontroll. Statens rätt reglerades länge av lagar från kolonialtiden, såsom the Indian Telegraph Act från 1885, som innebar stora möjligheter till att övervaka kommunikation. År 2000 antogs the Information Technology Act, som därefter åtföljts av diverse tillägg och regleringar. It-lagen ger den indiska staten makt att utifrån avsnitt 69A från 2008 års tillägg blockera information från allmänheten utifrån sex kriterier: ”suveränitet och integritet”, ”försvar av Indien”, ”statens säkerhet”, ”relationer med utländska stater”, ”allmän ordning” och för att motverka uppvigling till att begå brott relaterade till tidigare nämnda kriterier. Avsnitt 69A ger inte bara indiska myndigheter stora möjligheter att censurera innehåll på internet, utan också att bestraffa de som förmedlar informationen. Straffen kan sträcka sig från böter till sju års fängelse.[60] Den indiska statens försök att med lagstiftning kontrollera förmedlare av information på internet har tilltagit ytterligare bland annat genom antagandet av The Information Technology, Intermediary Guidelines and Digital Media Ethics Code Rules 2021.[61] Dessutom håller en ny it-lag på att beredas som ska fokusera på frågan om förmedlare av information. Förändringar under senare år tycks således i hög grad syfta till att ge staten starkare laglig grund för att blockera information för allmänheten, inte minst på USA-ägda digitala plattformar.

## Frihet, övervakning och informationsoperationer på internet

Indien uppfattas ofta som en demokrati, men saknar ett helt fritt internet. Freedom House kategoriserar internet i Indien som ”delvis fritt”, men med ett värde relativt nära begreppsklassen ”ofri”.[62] Indiska myndigheters agerande för att blockera innehåll på sociala medier har dessutom tilltagit under Modi-administrationens andra mandatperiod, 2019–2024, och förväntas fortsätta även därefter. Myndigheter har bland annat ökat kraven på amerikanska plattformar som X, YouTube, Instagram och Facebook, att blockera konton och inlägg. Information från Indiens myndighet för elektronik och informationsteknologi visar att Indien krävt att över 30 000 konton eller inlägg ska tas bort från amerikanska plattformar mellan 2020 och oktober 2023 med hänvisning till avsnitt 69A i den indiska it-lagen.[63] X har under senare år varit den främsta måltavlan för indiska krav.

En serie artiklar i *The Washington Post* under 2023 visar att X och andra plattformar från USA ofta har böjt sig för indiska myndigheters krav att ta bort användare och radera innehåll. Amerikanska plattformar har till exempel tagit bort konton och inlägg från BJP-kritiska individer och organisationer som arbetar för mänskliga

55 Ibid.

56 Anirudh Burman, ”Understanding India’s New Data Protection Law”, *Carnegie*, 3 oktober 2023.

57 Press Bureau of India, ”Government notifies DPDP Rules to empower citizens and protect privacy”, 14 november 2025.

58 Internet Freedom Foundation, ”IFF’s Initial Statement on the Notification of the Digital Data Protection Rules, 2025”, 14 november 2025. The Hindu, ”Too little, much later: on the Digital Personal Data Protection Rules, 2025”, 17 november 2025. Akhil Yadav ”India’s new data rules put the state above citizens”, IDR, 2 december 2025. Editors Guild of India, ”Statement on the Notified Rules Under the Digital Personal Data Protection Act”, 19 november 2025.

59 Sheikh Saaliq, ”India mandates pre-installation of government cyber safety app on all smartphones”, *AP*, 2 december 2025.

60 Ministry of Law, Justice and Company Affairs, Government of India, ”The Information Technology Act 2000”, 9 juni 2000; The Ministry of Law and Justice, ”The Information Technology (Amendment) Act 2008”, Government of India, 5 februari 2009.

61 Ministry of Electronics & Information Technology, Government of India, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

62 Freedom House, ”Freedom on the Net: India”, oktober 2024.

63 Ministry of Electronics and Information Technology, Government of India, ”Rajya Sabha Unstarred Question No. 732”.

rättigheter, men varit senfärdiga med att radera hindunationalistiska hatbudskap mot muslimer och desinformation från Indiens försvarsmakt.[64] Friheten på internet i Indien påverkas således negativt av att amerikanska företag anpassar sig till den alltmer restriktiva indiska lagstiftningen. Elon Musks motivering för plattformen X att ge efter för indiska krav lyder som följer:

> Vi måste respektera ett lands lagar annars kommer vår plattform att blockeras. / Om vi får ett domstolsbeslut och det domstolsbeslutet verkar vara i överensstämmelse med ett lands lagar, då vidtar vi de åtgärder som krävs, även om vi inte håller med om lagarna. / Bara om domstolsbeslutet verkar bryta mot ett lands lagar, som till exempel har hänt i Brasilien, bekämpar vi det.[65]

I mars 2025 lämnade dock X in en stämningsansökan till en domstol i Karnataka där Indiens inrikesdepartement anklagas för att i strid med nationell lagstiftning ha bemyndigat tjänstemän och upprättat en webbplats som leder till ”ohämmad censur av information”.[66]

Under 2018–2023 var Indien det land i världen som mest frekvent stängde ned internet, enligt Access Now. Organisationen menar att Indien stod för 116 av världens alla 283 nedsläckningar 2023.[67] Under 2024 stängde Indien av internet vid 84 tillfället, fler än alla andra länder, förutom Myanmar.[68] Nedsläckningarna uppges ha skett för att motverka våld mellan befolkningsgrupper, under demonstrationer och religiösa helgdagar, vid examinationer samt i samband med insatser mot brottsmisstänkta.[69] Under 2023 släckte indiska myndigheter ner internet i Manipur, en våldsdrabbad delstat med drygt tre miljoner invånare, i 212 dagar. Samma år stängde myndigheter också av internetuppkopplingen i Punjab, en delstat med nästan 30 miljoner invånare, under fyra dagar i följd, för att kunna gripa en sikhisk separatist.[70]

Mycket talar för att den BJP-styrda indiska staten även har använt internet för att övervaka meningsmotståndare, sprida desinformation och spionera utomlands. Avslöjanden indikerar att Indiens interna säkerhetstjänst, Intelligence Bureau, har köpt spionprogrammet Pegasus från israeliska NSO Group, som därefter använts för att övervaka ett stort antal indiska BJP-kritiska journalister, aktivister och politiker, bland dem oppositionsledaren Rahul Gandhi.[71] 2023 skickade Apple ut varningar till minst tjugo indiska journalister, politiker och forskare, om att statsstödda hackare angrep deras telefoner.[72] Indiens externa säkerhetstjänst, Research and Analys Wing (RAW), påstås också spridit desinformation utomlands. *The Washington Post* har exempelvis avslöjat att Disinfo Lab, ett tidigare populärt konto på X med så kallad grävande journalistik, drevs av en underrättelseofficer från RAW. Inlägg från Disinfo Lab, som delades brett av representanter från BJP, publicerade bland annat länkar till rapporter som påstår att George Soros motverkar indiska intressen och som beskriver BJP-kritiska röster i USA i mörk dager.[73]

Med undantag för Kanada är västerländska stater generellt försiktiga med att uttala sig kritiskt om Indien. Kanada påstår att RAW utfört mord i Kanada och att Indien utgör ett cyberhot mot nationen samt har försökt påverka kanadensiska val.[74] Kanadas nationella bedömande av cyberhot från 2024 pekar ut Indien som en motståndare tillsammans med Kina, Ryssland, Nordkorea och Iran, och menar att New Delhi troligen använder cyberdomänen för kontraterrorism, spionage och informationspåverkan.[75]

64 Joseph Menn och Gerry Shih, ”Under India’s pressure, Facebook let propaganda and hate speech thrive”, *The Washington Post*, 26 september 2023; Gerry Shih och Anant Gupta, ”Facing pressure in India, Netflix and Amazon back down on daring films”, *The Wasington Post*, 20 november 2023; Karishma Mehrotra och Joseph Menn, ”How India tamed Twitter and set a global standard for online censorship”, *The Washington Post*, 8 november 2023; Gerry Shih och Pranshu Verma, ”He live-streamed his attacks on Indian Muslims. YouTube gave him an award.”, *The Washington Post*, 26 september 2023.

65 Elon Musk, *X*, 2 maj 2024, hämtat 14 december 2024.

66 Reuters, ”X sues Modi’s government over content removal in new India censorship fight”, *The Guardian*, 20 mars 2025.

67 AccessNow, ”Unabashed and unabated: India leads the world shutdown count for sixth year”, 15 maj 2024; AccessNow, ”Shrinking Democracy, Growing Violence: Internet shutdowns in 2023”, maj 2024.

68 Access Now, ”Emboldened Offenders, Endangered Communities: Internet shutdowns in 2024”, februari 2025.

69 AccessNow, 15 maj 2024, 32–34.

70 Ibid, 32.

71 Sharad Vyas och Jurre van Bergen, ”Indian Spy Agency Bought Hardware Matching Equipment Used for Pegasus”, *Organized Crime and Corruption*, 20 oktober 22.

72 Gerry Shih, ”Apple warns Indian opposition and journalists of state-backed hacking”, 31 oktober 2023.

73 Gerry Shih, Clara Ence Morse och Pranshu Verma, ”Covert Indian operation seeks to discredit Modi’s critics in the U.S.”, *The Wasington Post*, 10 december 2023.

74 Philip Ling och Raffy Boudjikanian, ”India, Pakistan attempted to interfere in Canada’s elections: CSIS”, *CBS*, 5 april 2024.

75 Canadian Centre for Cyber Security, ”National Cyber Threat Assessment 2025–2026”, 2024, 8, 18.

## 5.4 Brics och Indiens ambitioner på internetområdet

Indiens regering strävar efter att göra Indien till en digital aktör att räkna med internationellt.[76] Utifrån mottot ”Digital India” vill Modi-administrationen bygga ut internetinfrastrukturen och genomdriva en digital omvandling av staten, ekonomin och samhället.[77] Indien vill också bli en ledande aktör (*leading power*) och ”hela världens guru” (*vishwaguru*), som formar globala normer, vilket även inkluderar den digitala domänen.[78] Det indiska utrikes- och säkerhetsetablissemanget lägger ett allt större fokus på cybersäkerhet. En första cybersäkerhetspolicy antogs 2013 och en nationell koordinator för cyberfrågor har tillsatts i Indiens nationella säkerhetsråd. Försvarsmakten stärker dessutom sin förmåga på området och antog 2024 en försvarsgrensgemensam försvarsdoktrin för operationer i cyberrymden.[79] Den tredje Modi-administrationen, som tillträdde 2024, framhåller vidare vikten av säkerhet på internet. I BJP:s valmanifest från 2024 betonas betydelsen av att ”säkerställa Indiens digitala suveränitet” och att ”implementera en robust cybersäkerhetspolicy”.[80] BJP utlovar att under mandatperioden 2024–2029 ”vidta stränga åtgärder mot digitala entiteter som hotar den indiska säkerheten på internet”, samt att ”reglera och se över Indiens myndigheter för cyberskydd och infrastruktur”.[81]

Indiens position i multilaterala institutioner, som FN och Brics, är ofta vag och svårtolkad. Trogen sin *multi alignment*-strategi är Indien medlem av både USA-initierade Group of Governmental Experts (GGE) och Ryssland-initierade Open-ended Working Group (OEWG) i FN. Forskaren Karthik Nachiappan menar, utifrån sin forskning om indisk förhandlingsteknik i multilaterala institutioner, att Indien fram till och med 2019 saknade en ”tydligt artikulerad position” i GGE och OEWG.[82] Indien har emellertid ibland uppfattats anta en hållning nära Ryssland, genom att inte acceptera de västliga ramverken The Paris Call for Trust and Security in Cyberspace och Budapestkonventionen om cyberbrottslighet, samt genom att ställa sig bakom ett ryskt initiativ på området.[83] Parallellt har emellertid Indien gått med i västdominerade *multi stakeholder*-initiativ, såsom the Global Partnership on Artificial Intelligence.[84]

Analytikern Sidharth Deb, som har analyserat officiella indiska inspel i FN, menar att Indien i vissa fall har framfört tydliga positioner, som i sin tur reflekterar den inrikespolitiska utvecklingen. Han hävdar att Indien i retoriken betonar vikten av *multi stakeholder*-initiativ, men i praktiken föredrar lösningar med staten i centrum. Deb drar också slutsatsen att Indien vill att innehåll i sociala medier faller under en breddad definition av cybersäkerhet samt att cyberterorrism blir en särskild kategori av cyberincidenter som kräver gemensamma internationella åtgärder. Han menar dessutom att Indien föredrar bindande internationella konventioner för reglering av internetområdet. Trots detta har Indien inte formulerat någon tydlig position om vad internationell rätt betyder på internetområdet, men däremot lyft frågor som rör tolkningen av begreppen jurisdiktion och suveränitet bortom territorialitet. 2021 tog Indien vidare upp frågan om vikten av privat informationsskydd på internet i OEWG. Enligt Deb handlade det framför allt om att understödja Indiens intressen att begränsa transnationella dataflöden för specifika syften och att effektivare kunna bedriva internationella brottsutredningar.[85]

Indien försöker också stärka sin roll ifråga om standarder inom Internationella teleunionen (ITU) inom FN. Under 2023 etablerade ITU ett regionalt kontor och innovationscentrum i New Delhi och 2024 var Indien värd för ITU:s World Telecommunication Standardization Assembly som hålls vart fjärde år. Indien har inom ramen för ITU gett förslag på resolutioner om standardisering av digital infrakultur och AI.[86] ITU har också anammat Indiens 5Gi som en av fyra teknologistandarder för 5G. 5Gi är en standalone-

76 Rajeev Chandrasekhar, ”Making India a digital power”, *MyGov,* 30 maj 2022.
77 Ministry of Electronics and Information Technology, ”Digital India: A programme to transform India into a digitally empowered society and knowledge economy”.
78 Neuman Bergenwall, *Indien som säkerhetspolitisk aktör*.
79 Ananya Raj Kakoti och Gunwant Singh, ”The new cyberspace doctrine’s impact on India’s security”, *Hindustan Times*, 13 juli 2024.
80 Bharatiya Janata Party, ”Modi ki Guarantee”, 2024.
81 Ibid.
82 Arindrajit Basu och Karthik Nachiappan, ”Will India negotiate in cyberspace?”, *Leidensecurityandglobalaffairsblog*, 16 december 2020.
83 Council of Europe, ”The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols”; Joyce Hakmeh och Allison Peters, ”Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet”, *Council on Foreign Relations*, 13 januari 2020.
84 The Global Partnership on Artificial Intelligence, ”Members”.
85 Sidharth Deb, ”Cyber Security at the UN: Where Does India Stand? (Part 2)”, *The CCG Blog*, 30 december 2021.
86 Press Information Bureau, Government of India, ”ITU-WTSA 2024 Concludes: India Leads the Charge for shaping the future of telecommunications/ICT with Global Backing for its pioneering resolutions in Telecommunications and Digital Innovation”, 24 oktober 2024.

version men utformad för att förbättra täckningen på landsbygden.[87]

Indiens vaga position när det gäller säkerhet och internet i multilaterala sammanhang gäller även för samarbetet inom Brics; under mötet i Kazan lyfte Jaishankar i sitt offentliga tal fram de indiska erfarenheterna av digitalisering, men gav ingen vägledning i var Indien står i frågor som rör säkerhet och internet.[88]

## 5.5 Slutsatser

För Indien är Brics framför allt ett verktyg för att höja sin status internationellt, stärka sin ekonomi och göra världsordningen mer multipolär. Syftet är inte att utveckla en anti-västlig allians. Indiens spända relationer till Kina och starka säkerhetspolitiska band till USA talar också emot ett djupt säkerhets- och it-samarbete inom Brics. En ytterligare komplicerande faktor är att indiska myndigheter förbjudit ett stort antal kinesiska applikationer och uteslutit kinesiska bolag från utbyggnaden av landet 5G-nät. Till det kommer att de indiska it-konsultföretagens tjänsteexport till USA och Europa är kritisk för Indiens ekonomi, vilket i sin tur stärker argumentet för ett öppet internet. Trots att Indien ofta framhåller suveränitetsprincipen begränsar inte dagens lagstiftning dataflöden över landets gränser. Däremot finns exempel på att Indien vidtagit åtgärder för att öka kontrollen över vilken information som får spridas inom landet, både genom att begära att information tas bort från plattformar och genom nedstängning av internet under perioder i regioner.

Några faktorer talar för att Indien skulle kunna vara öppet för ett djupare samarbete om internet inom Brics. Indien har trots konfliktfyllda relationer med Kina varit villigt att samarbeta om frågor som rör internetsäkerhet. De faktiska framsteg som skedde under 2024 om gränstvisten mellan Kina och Indien skulle potentiellt kunna leda till ett mer fruktbart samarbete inom Brics. Det kan även noteras att Kina är Indiens största handelspartner, att indiska och kinesiska bolag samäger nya undervattenskablar i Indiska oceanen och att tillverkare från Kina dominerar den indiska marknaden för smarta telefoner. Indiens hållning i FN tycks till viss del också ligga i linje med Rysslands perspektiv. Vidare har Indiens värdegemensamskap med Kina och Ryssland ökat i takt med att BJP genomfört inskränkningar i Indiens demokrati och minskat friheten på internet.

Så länge amerikanska företag ger efter för indiska myndigheters påtryckningar om censur är skälen svaga för Indien att liera sig med Brics-länderna om ett separat internet. Hur amerikanska it-jättar framöver hanterar Indiens krav på censur är en viktig fråga som inte bara kan påverka Brics-samarbetet utan också friheten på internet generellt. Fallet Indien skulle potentiellt kunna bli ett prejudikat för hur globala it-företag ska förhålla sig till auktoritära regeringars krav på blockeringar utifrån restriktiv nationell lagstiftning.

87 ITU, ”5G – Fifth generation of mobile technologies”.

88 Ministry of External Affairs, Government of India, ”Remarks by External Affairs Minister, Dr. S. Jaishankar at the BRICS Outreach Session in Kazan”, 24 oktober 2024.

# Referenser

3i Infrastructure. ”Global Cloud Xchange”, odaterad, hämtad 14 december, *https://www.3i-infrastructure.com/portfolio/current-portfolio/global-cloud-xchange*.

AccessNow. ”Shrinking Democracy, Growing Violence: Internet shutdowns in 2023”, maj 2024, hämtad 14 december 2024, *https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf*.

AccessNow. ”Unabashed and unabated: India leads the world shutdown count for sixth year”, 15 maj 2024, hämtad 10 december, *https://www.accessnow.org/press-release/india-keepiton-internet-shutdowns-2023-en*.

AccessNow. ”Emboldened Offenders, Endangered Communities: Internet shutdowns in 2024”, februari 2025, hämtad 12 december 2025, *https://www.accessnow.org/wp-content/uploads/2025/02/KeepItOn-2024-Internet-Shutdowns-Annual-Report.pdf*.

ANI. ”’Clearly, 30 countries saw value in it...’: Jaishankar commends BRICS at Munich Security Conference”, 17 februari 2024, hämtad 14 december 2024, *https://www.aninews.in/news/world/europe/clearly-30-countries-saw-value-in-it-jaishankar-commends-brics-at-munich-security-conference20240217204111*.

Barik, Soumyarendra. ”Data localisation, parental verification in data protection rules weigh most on tech industry’s minds”, *The Indian Express*, 15 januari 2025, hämtad 16 januari 2025, *https://indianexpress.com/article/business/data-protection-rules-verification-tech-industry-9778565*.

Barik, Soumyarendra. ”Draft Digital Personal Data Protection Rules, 2025: Committee for local data storage envisioned to prevent sectoral disruptions, says IT Minister”, *The Indian Express*, 6 januari 2025, hämtad 16 januari 2025, *https://indianexpress.com/article/business/draft-digital-personal-data-protection-rules-2025-committee-for-local-data-storage-envisioned-to-prevent-sectoral-disruptions-says-it-minister-9760275*.

Basu Arindrajit och Karthik Nachiappan. ”Will India negotiate in cyberspace?”, Leidensecurityandglobalaffairsblog, 16 december 2020, hämtad 14 december 2024, *https://www.leidensecurityandglobalaffairs.nl/articles/will-india-negotiate-in-cyberspace*.

Bharatiya Janata Party. ”Modi ki Guarantee”, 2024, hämtad 14 december 2024, *https://www.bjp.org/files/inline-documents/Modi-Ki-Guarantee-Sankalp-Patra-English_0.pdf*.

Burkhart, Grey E. et al. ”The Internet in India: Better Times Ahead?”. Communications of the ACM, vol. 41, nr. 11 (1998): 21–26.

Burman, Anirudh. ”Understanding India’s New Data Protection Law”, Carnegie, 3 oktober 2023, hämtad 14 december 2024, *https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en*.

Canadian Centre for Cyber Security. ”National Cyber Threat Assessment 2025-2026”, hämtad 14 december 2024, *https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf*.

Chakraborty, Abhishek och Reuters, ”Starlink In India Soon? Elon Musk Takes On Mukesh Ambani’s Reliance Jio”, NDTV, 12 november 2024, hämtad 15 januari 2025, *https://www.ndtv.com/world-news/starlink-in-india-soon-elon-musk-takes-on-mukesh-ambanis-reliance-jio-7003416*.

Chandrasekhar, Rajeev. ”Making India a digital power”, MyGov, 30 maj 2022, hämtad 14 december 2024, *https://blog.mygov.in/editorial/making-india-a-digital-power*.

Chaudhuri, Rudra och Arjun Kang Joseph. ”Living in a fragmented world: India’s data way”, *India Review*, vol. 23, nr. 2 (2020): 154–76.

Chaudhuri, Rudra, och Nabarun Roy. ”India and the sovereignty principle: the disaggregation imperative”, *India Review*, vol 23, nr 2 (2024): 89–94.

Council of Europe. ”The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols”, hämtad 14 december, *https://www.coe.int/en/web/cybercrime/20th-anniversary-budapest-convention*.

Deb, Sidharth. ”Cyber Security at the UN: Where Does India Stand? (Part 2)”, The CCG Blog, 30 december 2021, hämtad 14 december 2024, https://ccgnludelhi.wordpress.com/2021/12/30/cyber-security-at-the-un-where-does-india-stand-part-2.

Department of Telecommunications, Ministry of Communications, Government of India. ”Auction_2022_Bid_Ranking”, 5 september 2022, hämtad 15 januari 2025, *https://dot.gov.in/sites/default/files/Auction_2022_Bid_Ranking.pdf*.

Department of Telecommunications, Ministry of Communications, Government of India. ”Auction_2024_Bid_Ranking”, 17 september 2024, hämtad 15 januari 2025, *https://dot.gov.in/sites/default/files/25%20Auction_2024_Bid_Ranking.pdf*.

Editors Guild of India. ”Statement on the Notified Rules Under the Digital Personal Data Protection Act”, 19 november 2025, hämtad 12 december 2025, *https://editorsguild.in/statements-issued*.

EKN. ”Record deal behind record-time 5G rollout in India”, 7 november 2023, hämtad 14 december 2024, *https://www.ekn.se/en/ekn-magazine/ekns-magazine/record-deal-behind-record-time-5g-rollout-in-india*.

Freedom House. ”Freedom on the Net: India”, Washington, DC: Freedom House, 2024, hämtad 29 oktober 2024, *https://freedomhouse.org/country/india/freedom-net/2024*.

Goldman Sachs. “How India’s services economy became a world leader”, 13 januari 2024, hämtad 31 oktober 2024, *https://www.goldmansachs.com/insights/articles/how-india-services-economy-became-a-world-leader*.

Gonzalo, Manuel, et al. “5G Kick-off in India and Brazil: InterState Competition, National Systems of Innovation, and Catch-up Implications for the Global South”, Seoul Journal of Economics, vol. 36, nr. 1 (2023): 53–78.

Hakmeh, Joyce, och Allison Peters. ”Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet”, Council on Foreign Relations, 13 januari 2020, hämtad 12 december 2025, *https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet*.

Haque, Ehtesham. ”Satellite internet showdown: Starlink vs Jio and what’s best for India’s future”, T*he Times of India*, 16 oktober 2024, hämtad 15 januari 2025, *https://timesofindia.indiatimes.com/blogs/thebigd/satellite-internet-showdown-starlink-vs-jio-and-whats-best-for-indias-future*.

IANS. ”Jio only one to not use Chinese components: Mukesh Ambani told Donald Trump”, Mint, 28 februari 2020, hämtad 14 december 2024, *https://www.livemint.com/industry/telecom/jio-only-one-to-not-use-chinese-components-mukesh-ambani-told-trump-11582866113641.html*.

ICRA. ”India’s data centre operational capacity to double in next 30 months to 2,000–2,100 MW by FY2027”, 22 oktober 2024, hämtad 15 december 2024, *https://www.icra.in/CommonService/OpenMediaS3?Key=b08638cb-2a72-433a-8406-3778bc208a75*.

IDC. ”Indian PC Market Grew 7.1% YoY with 3.39 Million Units Shipped in 2Q2024, says IDC”, 19 augusti 2024, hämtad 14 december 2024, *https://www.idc.com/getdoc.jsp?containerId=prAP52532224*.

IDC. ”Indian Smartphone Market Grew 7% YoY in 1H24, Reaching 69 Million Units”, 13 augusti 2024, hämtad 14 december 2024, *https://www.idc.com/getdoc.jsp?containerId=prAP52521824*.

Internet Society Pulse. ”IXP Tracker: India”, hämtad 15 december 2024, *https://pulse.internetsociety.org/en/ixp-tracker/?country_code=IN*.

Internet Freedom Foundation. ”IFF’s Initial Statement on the Notification of the Digital Data Protection Rules, 2025”, 14 november 2025, hämtad 12 december 2025, *https://internetfreedom.in/iffs-initial-statement-on-the-notification-of-the-digital-data-protection-rules-2025.*

ITU. ”5G – Fifth generation of mobile technologies”, augusti 2024, hämtad 15 januari 2025, *https://www.itu.int/en/mediacentre/backgrounders/Pages/5G-fifth-generation-of-mobile-technologies.aspx*.

Ling, Philip, och Raffy Boudjikanian. ”India, Pakistan attempted to interfere in Canada’s elections: CSIS”, CBS, 5 april 2024, hämtad 14 december 2024, *https://www.cbc.ca/news/politics/pakistan-india-elections-canada-1.7164378*.

Malone, David, et al. *The Oxford Handbook of Indian Foreign Policy*. Oxford: Oxford University Press, 2015.

Mehrotra, Karishma, och Joseph Menn. ”How India tamed Twitter and set a global standard for online censorship”, *The Washington Post*, 8 november 2023., hämtad 14 december 2024, *https://www.washingtonpost.com/world/2023/11/08/india-twitter-online-censorship*.

Menn, Joseph, och Gerry Shih. ”Under India’s pressure, Facebook let propaganda and hate speech thrive”, *The Washington Post*, 26 september 2023, hämtad 14 december 2024, *https://www.washingtonpost.com/world/2023/09/26/india-facebook-propaganda-hate-speech*.

Ministry of Electronics & Information Technology, Government of India. ”Software Technology Parks of India (STPI)”, odaterad, hämtad 14 december 2024, *https://www.meity.gov.in/content/stpi*.

Ministry of Electronics & Information Technology, Government of India. ”The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021”, 6 april 2023, hämtad 14 december 2024, *Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf.*

Ministry of Electronics and Information Technology. ”Digital India: A programme to transform India into a digitally empowered society and knowledge economy”, odaterad, hämtad 14 december 2024, *https://www.meity.gov.in/sites/upload_files/dit/files/Digital%20India.pdf*.

Ministry of Electronics and Information Technology, Government of India, “Rajya Sabha Unstarred Question No. 732”, hämtad 14 december 2024. *https://sansad.in/getFile/annex/262/AU732.pdf?source=pqars*.

Ministry of External Affairs, Government of India. ”Remarks by External Affairs Minister, Dr. S. Jaishankar at the BRICS Outreach Session in Kazan”, 24 oktober 2024, hämtad 14 december 2024, *https://www.mea.gov.in/Speeches-Statements.htm?dtl/38461/Remarks_by_External_Affairs_Minister_Dr_S_Jaishankar_at_the_BRICS_Outreach_Session_in_Kazan*.

Ministry of Law, Justice and Company Affairs, Government of India. ”The Information Technology Act 2000”, 9 juni 2000, hämtad 14 december 2024, *https://www.meity.gov.in/writereaddata/files/itbill2000.pdf*.

Mishra, Rahul. ”From non-alignment to multi-alignment: assessing India’s foreign policy shift”. The Round Table: The Commonwealth Journal of International Affairs, vol. 112, nr 1 (2023): 43–56.

Mukherjee, Vaddha. ”Chinese smartphone giants seek Indian partnerships amid govt push”, Business Standard, 4 juli 2024, hämtad 29 oktober 2024, *https://www.business-standard.com/industry/news/chinese-smartphone-giants-seek-indian-partnerships-amid-govt-push-124070400373_1.html*.

Musk, Elon. X, 2 maj 2024, hämtad 14 december 2024, *https://x.com/elonmusk/status/1786072713766855143*.

National Informatics Centre, Government of India. ”NICNET”, odaterad, hämtad 6 december 2024, *https://www.nic.in/servicecontents/nicnet*.

Neuman Bergenwall, Samuel. *Indien som säkerhetspolitisk aktör: konsekvenser för svenska försvarsrelationer*. FOI-R--5588--SE. Stockholm: FOI, 2024.

Nokia. ”Nokia wins multi-billion 5G extension deal from Bharti Airtel for its India operations”, odaterad, hämtad 14 december 2024, *https://www.nokia.com/about-us/news/releases/2024/11/20/nokia-wins-multi-billion-5g-extension-deal-from-bharti-airtel-for-its-india-operations*.

Observer Research Foundation. ”To Us, They Serve Different Purposes: EAM Jaishankar on India’s BRICS & QUAD Diplomacy”, YouTube, 7 november 2024, hämtad 14 december 2024, *https://www.youtube.com/watch?v=--Z3pfKFQsg*.

Panda, Jagannath. ”India’s BRICS Balancing Act”, 17 oktober 2024. United States Institute for Peace, hämtad 14 december 2024, *https://www.usip.org/publications/2024/10/indias-brics-balancing-act*.

Pandey, Kamya. ”Battle lines drawn for regulating Internet Exchange Points in India: Extreme and NIXI vs Vodafone Idea”, Medianama, 28 november 2024, hämtad 15 december 2024, *https://www.medianama.com/2024/11/223-ixp-regulation-extreme-ix-nixi-vs-vodafone-idea*.

Pant, Harsh V., red. ”From BRICS to BRICS Plus: Old Partners and New Stakeholders,” ORF Special Report No. 214, Observer Research Foundation, september 2023, hämtad den 13 december. *https://www.orfonline.org/public/uploads/posts/pdf/20231229212147.pdf*.

Pant, Harsh V. och Rajoli Siddharth Jayaprakash. ”In Kazan, the Global South makes a point about Brics”, The Hindustan Times, 24 oktober 2024, hämtad 14 december 2024, *https://www.hindustantimes.com/opinion/in-kazan-the-global-south-makes-a-point-about-brics-101729782078812.html*.

Press Bureau of India, Ministry of Education. ”Shri Dharmendra Pradhan with Shri Ashwini Vaishnaw successfully tests the ‘BharOS’, a Made in India mobile operating system developed by IIT Madras”, 24 januari 2023, hämtad 14 december 2024, *https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1893230*.

Press Bureau of India, Ministry of Electronics & IT. ”Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order”, 29 juni 2020, hämtad 14 december 2024, *https://pib.gov.in/PressReleasePage.aspx?PRID=1635206*.

Press Information Bureau, Government of India. ”ITU-WTSA 2024 Concludes: India Leads the Charge for shaping the future of telecommunications/ICT with Global Backing for its pioneering resolutions in Telecommunications and Digital Innovation”, 24 oktober 2024, hämtad 15 januari 2025, *https://pib.gov.in/PressReleseDetailm.aspx?PRID=2067905&reg=3&lang=1*.

Press Bureau of India. ”Government notifies DPDP Rules to empower citizens and protect privacy”, 14 november 2025, hämtad 12 december 2025, *https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190014&reg=3&lang=2*.

Press Information Bureau, Government of India. ”Universal connectivity and Digital India initiatives reaching to all areas, including tier-2/3 cities and villages”, 2 augusti 2024, hämtad 13 december 2024, *https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2040566*.

Press Trust of India. ”Software services export grows to $205.2 bn in FY24, US major destination”, Business Standard, 18 oktober 2024, hämtad 14 december, *https://www.business-standard.com/industry/news/software-services-export-grows-to-205-2-bn-in-fy24-us-major-destination-124101801218_1.html*.

Press Trust of India. ”Elon Musk’s Starlink gets licence to start India services amid feud with Trump”, The Hindu, 6 juni 2025, hämtad 12 december 2025, *https://www.thehindu.com/business/Industry/elon-musks-starlink-gets-licence-to-start-india-services-amid-feud-with-trump/article69665198.ece*.

Raj Kakoti, Ananya och Gunwant Singh. ”The new cyberspace doctrine’s impact on India’s security”, H*industan Times*, 13 juli 2024, hämtad 30 november 2024, *https://www.hindustantimes.com/ht-insight/future-tech/the-new-cyberspace-doctrine-s-impact-on-indias-security-101720843641057.html*.

Ranjan Sen, Sudhi. ”Modi Says BRICS Must Avoid Being an Anti-West Group as It Grows”, *Bloomberg*, 24 oktober 2024, hämtad 14 december 2024, *India PM Modi Says BRICS Must Avoid Being an Anti-West Group as It Grows - Bloomberg*.

Saaliq, Sheikh. ”India mandates pre-installation of government cyber safety app on all smartphones”, AP, 2 december 2025, hämtad 12 december 2025, *https://apnews.com/article/india-sanchar-app-privacy-cyber-b2564204c6eda0c620e9c293d94f9839*.

SCB. ”Befolkning, antal efter födelseland och år”, Statistikdatabasen, hämtad 15 januari 2025, *https://www.statistikdatabasen.scb.se/pxweb/sv/ssd/START__BE__BE0101__BE0101E/FodelselandArK*.

Sha, Arjun. ”5G Bands Supported in India: Everything You Need to Know”, *Beebom*, 28 januari 2022, hämtad 16 jaunari 2025, *https://beebom.com/5g-bands-india*.

Shih, Gerry. ”Apple warns Indian opposition and journalists of state-backed hacking”, *The Washington Post*, 31 oktober 2023, hämtad 14 december 2024, *https://www.washingtonpost.com/world/2023/10/31/india-phone-hacking-apple*.

Shih, Gerry, et al. ”Covert Indian operation seeks to discredit Modi’s critics in the U.S.”, *The Wasington Post*, 10 december 2023, hämtad 14 december 2024, *https://www.washingtonpost.com/world/2023/12/10/india-the-disinfo-lab-discredit-critics*.

Shih, Gerry, och Anant Gupta. ”Facing pressure in India, Netflix and Amazon back down on daring films”, *The Wasington Post*, 20 november 2023, hämtad 14 december 2024, *https://www.washingtonpost.com/world/2023/11/20/india-netflix-amazon-movies-self-censorship*.

Shih, Gerry, och Pranshu Verma. ”He live-streamed his attacks on Indian Muslims. YouTube gave him an award”, *The Washington Post*, 26 september 2023., hämtad 14 december 2024, *https://www.washingtonpost.com/world/2023/09/26/india-monu-manesar-viligante-social-media*.

Similarweb. ”Top Apps Ranking: India”, odaterad, hämtad 14 december 2024, *https://www.similarweb.com/top-apps/google/india*.

Software Technology Parks of India, Ministry of Electronics & Information Technology, Government of India. ”Data Center: STPI’s Tier-III Data Centers”, odaterad, hämtad 15 december 2024, *https://stpi.in/en/data-center*.

Submarine Cable Map. ”India”, odaterad, hämtad 6 december 2024, *https://www.submarinecablemap.com/country/india.*

Submarine Cable Networks. ”India”, odaterad, hämtad 29 oktober 2024, *https://www.submarinenetworks.com/en/stations/asia/india*.

Telecom Regulatory Authority of India. ”Consultation Paper on The Terms and Conditions of Network Authorisations to be Granted Under the Telecommunications Act, 2023”, Consultation Paper No. 16/2024, 22 oktober 2024, hämtad 15 december 2024, *https://www.trai.gov.in/sites/default/files/CP_22102024.pdf*.

Telecom Regulatory Authority of India. ”The Indian Telecom Services: Yearly Performance Indicators 2023–2024”, 14 augusti 2024, hämtad 13 december 2024, *https://www.trai.gov.in/sites/default/files/Report_14082024.pdf*.

Telecom Regulatory Authority of India. ”The Indian Telecom Services: Yearly Performance Indicators 2023–2024”, 14 augusti 2024, hämtad 13 december 2024, *https://www.trai.gov.in/sites/default/files/Report_14082024.pdf*.

Telecomelead. ”India’s used smartphone market grows amid challenges in new device sales”, 16 oktober 2024, hämtad 14 december 2024, *https://telecomlead.com/smart-phone/indias-used-smartphone-market-grows-amid-challenges-in-new-device-sales-118538*.

Tellis, Ashley J. ”Non-Allied Forever: India’s Grand Strategy According to Subrahmanyam Jaishankar”, Carnegie, 3 mars 2021, hämtad den 14 december 2024, *https://carnegieendowment.org/posts/2021/03/non-allied-forever-indias-grand-strategy-according-to-subrahmanyam-jaishankar?lang=en*.

The Hindu. ”Too little, much later: on the Digital Personal Data Protection Rules, 2025”, 17 november 2025, hämtad 17 november 2025, *https://www.thehindu.com/opinion/editorial/too-little-much-later-on-the-digital-personal-data-protection-rules-2025/article70287191.ece*.

The Economic Times. ”21 Indian-origin CEOs of billion dollar companies”, 29 november 2023, hämtad 14 december 2024, *https://economictimes.indiatimes.com/nri/work/sundar-pichai-satya-nadella-ajay-banga-arvind-krishna-and-20-other-indian-origin-ceos-of-billion-dollar-companies/sundar-pichai/slideshow/105593531.cms*.

The Global Partnership on Artificial Intelligence. ”Members”, odaterad, hämtad 14 december 2024, *https://gpai.ai/community*.

The Ministry of Law and Justice. ”The Information Technology (Amendment) Act 2008”, Government of India, 5 februari 2009, hämtad 14 december 2024, *https://www.meity.gov.in/writereaddata/files/itbill2000.pdf*.

Times of India. ”Big Boost for India’s internet quality! Three large undersea cable projects to expand capacity by more than four times”, 21 augusti 2024, hämtad 14 december 2024, *https://timesofindia.indiatimes.com/business/india-business/big-boost-for-indias-internet-quality-three-large-undersea-cable-projects-to-expand-capacity-by-more-than-four-times/articleshow/112672969.cms*.

Times of India. ”BSNL India’s first direct-to-direct-device satellite service: What it means for users, key features and more”, 15 november 2024, hämtad 15 januari 2025, *http://timesofindia.indiatimes.com/articleshow/115326722.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst*.

Vyas, Sharad och Jurre van Bergen. ”Indian Spy Agency Bought Hardware Matching Equipment Used for Pegasus”, Organized Crime and Corruption, 20 oktober 22, hämtad 14 december 2024, *https://www.occrp.org/en/news/indian-spy-agency-bought-hardware-matching-equipment-used-for-pegasus*.

Världsbanken. ”Trade in services (% of GDP) – India”, hämtat 17 februari 2026, https://data.worldbank.org/indicator/BG.GSR.NFSV.GD.ZS?locations=IN.

Yadav, Akhil. ”India’s new data rules put the state above citizens”, IDR, 2 december 2025, hämtad 12 december 2025, *https://idronline.org/article/rights/indias-new-data-rules-put-the-state-above-citizens*.

# 6. Kina – cyberstormakten i Brics

*Per-Erik Nilsson*

*Att bygga Kina till en 'cyberstormakt' är ett långsiktigt, komplext och systematiskt strategiskt projekt som omfattar alla aspekter av ekonomin och samhället.*

Chen Zhaoxiong, biträdande minister vid Ministeriet för industri och informationsteknologi, 2017.[1]

## 6.1 Kinas relation med Brics

Kina har varit med i Brics sedan grunden lades 2005 när Ryssland höll det första RIC-mötet med Indien och Kina. För Kina är Brics en arena för multilateralt samarbete i en tid av ökande multipolaritet.[2] Det handlar om att främja den egna ekonomin och industrin samt att stärka sitt diplomatiska inflytande. Brics framstår som en naturlig förlängning av en lång tradition av kinesisk utrikespolitik med fokus på att forma allianser och nätverk i det globala syd för att erbjuda ett alternativ till den västledda ordningen.[3] Som den ekonomiskt starkaste parten i organisationen har Kina stort inflytande.[4] Brics-ländernas ideologiska brokighet och till viss del konfliktartade relationer gör dock att Peking inte har sett organisationen som ett enskilt alternativ för att driva sina internationella agendor. Andra viktiga kinesiska samarbetsinitiativ är Asiatiska infrastrukturinvesteringsbanken och Shanghaisamarbetet.[5]

Beträffande Brics interna stridigheter är Kinas relation med Brics näst största ekonomi, Indien, central. Trots en långvarig gränskonflikt har Kina tillsammans med Ryssland drivit en antivästlig linje och förespråkat en omfattande utvidgning av Brics för ökad export till, och inflytande i, utvecklingsländer. Detta är något som Indien har motsatt sig, delvis för att bibehålla goda relationer med väst, delvis för att inte marginaliseras av nya Bricsmedlemmar som är lojala med Peking.[6] Efter Bricsmötet i Kazan 2024 publicerade det kinesiska Utrikesdepartementet en mötesrapport där Kinas och Indiens relation behandlades. Den betonade att länderna ska inta ett "strategiskt och långsiktigt perspektiv, förhindra att specifika meningsskiljaktigheter påverkar den övergripande relationen" för att "upprätthålla regional och global fred och välstånd och främja en multipolär värld".[7]

Trots många utfästelser om politiska åtaganden, ekonomiskt samarbete och potential för kinesiska direktinvesteringar (2009–2019) i de andra Bricsländerna, visar en analys att den faktiska intensifieringen av investeringar har varit begränsad, vilket påvisar en skillnad mellan retorik och verklighet.[8] Ett Brics som expanderar i enlighet med Kinas vision tillsammans med ökade spänningar mellan Kina och USA skulle dock kunna leda till ett mer integrerat Brics där Kina kommer att spela en avgörande roll, inte minst på cyberområdet.

## 6.2 Internets utveckling i Kina

Kina kopplades upp på det globala internet 1994 med internets grundläggande protokoll TCP/IP. Under 1980-talet hade Peking framhållit vikten av att utveckla landets it-infrastruktur, vilket ledde till lanseringen av

1 Citerad i: Rush Doshi, m.fl., *China as a "Cyber Great Power": Beijing's Two Voices in Telecommunications* (Washington: Brookings, 2021), 5.

2 Se exempelvis Hu Jintaos tal under under det tredje Brics-mötet 2011, i Utrikesdepartementet, "Hu Jintao Presides over and Delivers an Important Speech at the Third BRICS Leaders Meeting in Sanya, Hainan Province", Kinas folkrepublik, 14 april 2011.

3 Brice Tseen Fu Lee och Juan Pablo Sims, "Legitimacy Through Diversity: China's Leadership in the BRICS + Expansion for Global Balance", *Fudan Journal of the Humanities and Social Sciences*, online first (2024): 1–38; Guangyu Qiao-Franco, "An Emergent Community of Cyber Sovereignty: The Reproduction of Boundaries?", *Global Studies Quarterly*, vol. 4, nr. 1 (2024): 1–11, 5.

4 Bas Hooijmaaijers, "China, the BRICS, and the Limitations of Reshaping Global Economic Governance", *The Pacific Review*, vol. 34, nr. 1 (2021): 29–55.

5 Se Joseph Y. S. Cheng, "China's Approach to BRICS", *Journal of Contemporary China*, vol. 24, nr. 92 (2015): 357–75.

6 Se vidare Hung Tran, "China and India Are at Odds Over BRICS Expansion", *Atlantic Council*, 8 augusti 2023.

7 Utrikesdepartementet, "President Xi Jinping Meets with Indian Prime Minister Narendra Modi", Folkrepubliken Kina, 24 oktober 2024.

8 Bas Hooijmaaijers, "The BRICS Countries' Bilateral Economic Relations, 2009 to 2019: Between Rhetoric and Reality", *Sage Open,* vol. 11, nr. 4 (2021): 1–16.

863-programmet 1986.[9] Programmet syftade till att komma i kapp västs teknologiska och tekniska försprång genom att modernisera vetenskap och industri.[10] År 1997 deklarerade Youjin Zheng, direktören för landets Centrum för informationsinfrastruktur:

> Informatisering är grunden till Kinas ekonomiska modernisering; informationsresurser är bland de mest basala och viktiga aspekterna för modern ekonomisk utveckling; informationsindustrin borde bli en fundamental sektor i Kinas ekonomi.[11]

När Kina anslöt till det globala internet var landets *fysiska lager* (se kapitel 2) eftersatt jämfört med industrialiserade länder, men detta gjorde att Kina kunde bygga en infrastruktur anpassad till den kommande internetbaserade globaliseringen.[12] Redan 1998 hade landet ett nationellt nätverk av fiberkabel som kopplade samman alla provinser och större städer.[13]

1996 delade det kinesiska statsrådets förordning nr. 195 upp det kinesiska internet i två kategorier – i *sammankopplade nätverk* direkt kopplade till det globala internet och i *accessnät* (eller tillgångsnät) som kopplade slutanvändare till större nätverk i Kina. De sammankopplade nätverken kontrollerades av fyra statliga organ vilka tillhandahöll licenser till internetleverantörer.[14] Tillgångsnätverken var friare och verkade på en öppnare marknad. De fick dock inte koppla upp sig mot det globala internet utan tillstånd. Detta gav den kinesiska regeringen omfattande kontroll över tillgång och distribution av internet i Kina.[15] För att kontrollera den snabbt expanderande utvecklingen skapades 1998 Ministeriet för informationsindustri, som blev en av Kinas främsta tillsynsmyndigheter för internet. Ministeriet fick ökat mandat och omvandlades 2008 till Ministeriet för informationsindustri och teknik.[16]

Under 2000-talet ökade antalet internet- och mobiltelefonanvändare snabbt. 2008 hade 253 miljoner invånare tillgång till internet och två år senare 457 miljoner.[17] År 2000 hade Kinas mobiltelefonimarknad passerat USA:s och blivit den största i världen.[18]

Kommunistpartiets satsningar på digital utveckling fortsatte med ”Planen för medel- och långsiktig vetenskaplig och teknisk utveckling 2006–2020”, som betonade vikten av inhemsk innovation, även kallat Kinas ”teknonationalism”.[19] Denna strategi innebar att Kina strategiskt använde utländska investeringar och internetglobalisering för att utveckla inhemsk industri.[20] Exempelvis begränsades utländska bolags handlingsutrymme på den inhemska kinesiska marknaden. Vidare fick kinesiska företag stort handlingsutrymme att göra utländska investeringar, samtidigt som styret i Peking valde att inte upprätthålla sina lagar mot utländsk bestickning, vilket i praktiken möjliggjorde att statliga bolag kunde använda mutor i internationella affärer.[21] Till detta ska även läggas Kinas historia av att införskaffa utländsk teknologi och teknik via både legala

9 Namnet syftar till datumet för lanseringen av programmet och kommer från det kinesiska sättet att skriva årtal och månader: 86 (1986) och 3 (mars).

10 Programmet omfattade de så kallade Gyllene projekten: Den gyllene bron (digitalt informationsutbyte), Det gyllene kortet (digitala betaltjänster) och Den gyllene skatten (digital beskattning). I samband med dessa introducerades även Den gyllene skölden (också kallad den Stora brandväggen, som idag utgör Kinas internetcensur. Se: Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* (Santa Barbara: Praeger, 2017), 5; Xiudian Dai, ”ICTs in China's Development Strategy”, i *China and the Internet: Politics of the Digital Leap Forward*, red. Christopher R. Hughes och Gudrun Wacker (London och New York: Routledge, 2003), 10.

11 Zheng i Gianluigi Negro, *The Internet in China: From Infrastructure to Nascent Civil Society* (Cham: Palgrave Macmillan, 2017), 21.

12 Rogier Creemers, ”The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy”, *Journal of Contemporary China*, vol. 33, nr. 146 (2024): 173–88, 175.

13 Dai, ”ICTs in China's”, 13.

14 Nätverken: China Education and Research Network (CERNET) etablerades 1994 med Utbildningsministeriet som kontrollorgan; China Science and Technology Network (CSTNet) etablerades 1994 med Kinesiska vetenskapsakademin som kontrollorgan; ChinaNET etablerades 1994 med telekombolaget China Telecom som kontrollorgan; China Golden Bridge Network (China GBN) etablerades 1996 med Ministeriet som för post och telekommunikation och sedermera Ministeriet för industri och informationsteknik som kontrollorgan.

15 Negro, *The Internet in China*, 29–30.

16 Negro, *The Internet in China*, 26.

17 Tianjiao Jiang, ”The Shift of China's Strategic Thinking on Cyberwarfare Since the 1990s”, *Journal of Chinese Political Science*, vol. 28, nr. 1 (2023): 127–49, 135.

18 Zixue Tai, *The Internet in China: Cyberspace and Civil Society* (London och New York: Routledge, 2006), 119.

19 Se exempelvis Tai Ming Cheung, ”The Rise of China as a Cybersecurity Industrial Power: Balancing National Security, Geopolitical, and Development Priorities”, *Journal of Cyber Policy*, vol. 3, nr. 3 (2018): 306–26; Yongwoon Shim och Dong-Hee Shin, ”Neo-Techno Nationalism: The Case of China's Handset Industry”, *Telecommunications Policy*, vol. 40, nr. 2–3 (2016): 197–209.

20 Cheung, ”The Rise of China”, 308.

21 Daniel C. K. Chow, ”How China Promotes Its State-Owned Enterprises at the Expense of Multinational Companies Doing Business in China and in other Countries”, Ohio State Public Law Working Paper, nr. 307: 1–29.

och olagliga metoder, som industrispionage.[22] Utöver detta är det väl känt att Kina producerar och monterar en stor del av teknikvaror för västerländska tillverkare. Det har dock inte enbart handlat om att utnyttja billig arbetskraft. Som exempel har det amerikanska teknikföretaget Apple under drygt två decennier koncentrerat sin tillverkning i Kina och därigenom möjliggjort en omfattande kunskapsöverföring som indirekt bidragit till landets teknologiska utveckling och tekniska expertis. I praktiken har Apple tränat och utbildat tusentals designers, ingenjörer, chefer och it-specialister. Mellan 2016 och 2021 investerade bolaget dessutom omkring 275 miljarder dollar i Kina och skapade runt fem miljoner arbetstillfällen. Detta har dock försatt Apple, liksom andra västerländska teknikbolag, i en djup beroendeställning till Kina.[23]

Under 2010-talet skedde framväxten av stora kinesiska teknik-, telekom- och e-handelsbolag som Baidu, Alibaba och Tencent, samt teknikbolag som Huawei och Xiaomi som erhöll stora marknadsandelar utomlands.[24] Ett annat framgångsrikt exempel är ByteDance som med den digitala plattformen TikTok kom att bli en av de globalt mest använda.[25] Till detta ska läggas även en rad andra nischade teknikbolag som har främjats av den kinesiska staten. Det gäller exempelvis teknik för ansiktsigenkänning, bildigenkänning, autonomona fordon, med mera.[26]

Ett knappt decennium efter att planen om medel- och långsiktig teknisk utveckling hade introducerats, presenterade premiärministern Li Keqiang den nya handlingsplanen ”Internet plus” (2015) för att stärka ekonomi och industri genom teknologisk och teknisk innovation.[27] I samband med handlingsplanen presenterades även strategin ”Tillverkat i Kina 2025” som satte mål för tio strategiska sektorer för att befästa Kinas position som ledande aktör i en digitaliserad framtid.[28] 2017 introducerades Kinas första plan för artificiell intelligens, syftande till att skapa ett heltäckande AI-ekosystem.[29]

Sedan 1980-talet har styret i Peking satsat på att komma ikapp länder med ett tekniskt försprång inom it och internet. Statliga och privata initiativ har gradvis stärkt Kinas roll som en ledande cybernation i både det *fysiska och det logiska lagret* (se kapitel 2), vilket inte minst syns i en remarkabel utveckling i ansökta patent. Det ska dock understrykas att kvantitet inte är ett bevis för kvalitet. Kina har kritiserats för att lämna in patent av dålig kvalitet vilket också kan antas bevisas i det faktum att relativt få patent leder till innovation i jämförelse med andra ledande aktörer.[30] I anslutning till utvecklingen inom de fysiska och logiska lagren bör även framväxten av tekniska innovationer i det översta användar- eller innehållslagret uppmärksammas. Särskilt relevant är de system som kopplas till landets kreditsystem, vilka utgör instrument för finansiell och social styrning genom insamling, sammanställning och användning av data, snarare än ett enhetligt och centraliserat poängsystem.[31]

Den här utvecklingen har möjliggjorts av en rad faktorer, bland andra: god tillgång till finansiering av tekniksektorn via lån, investeringar och riskkapital; en balans mellan statlig kontroll och innovationsfrihet via kommunistpartiets femårsplaner som har satt långsiktiga mål utan att detaljstyra ekonomin och industrin; en enorm inhemsk marknad för produktvalidering och som präglas av hård konkurrens; aggressiva metoder för

22 Se exempelvis William C. Hannas och Huey-Meei Chang, ”Chinese Technology Transfer”, i *China's Quest for Foreign Technology: Beyond Espionage*, red. William C. Hannas och Didi Kirsten Tatlow (London och New York: Routledge, 2021), 3–21; Tim Rühlig, *The Sources of China's Innovativeness Why China's ”Unstoppable” Innovation Powerhouse Might Falter*, DGAP Analysis (Berlin: German Council of Foreign Relations, 2023).

23 Se Patrick McGee, *Apple in China: The Capture of the World's Greatest Company* (London and New York: Simon and Schuster, 2025).

24 För en kort historik om bolagen, se Dominique Jolly, *The New Threat: China's Rapid Technological Transformation* (Cham: Palgrave Macmillan, 2022), 75ff; Hong Shen, *China's Tech Giants: Baidu, Alibaba, Tencent* (Bonn och Berlin: Konrad Adenauer Stiftung, 2018).

25 Om ByteDance och TikTok, se Majdouline Mhalla, Jiang Yun och Alireza Nasiri, ”Video-Sharing Apps Business Models: TikTok Case Study”, *International Journal of Innovation and Technology Management*, vol. 17, nr. 7 (2020): 1–25.

26 Se Mattias Burell och Kristina Sandklef, *AI-Utvecklingen i Kina – Påverkan på den svenska tjänstemannasektorn* (Stockholm: Futurion, 2022).

27 Yu Hong, ”Pivot to Internet Plus: Molding China's Digital Economy for Economic Restructuring?”, *International Journal of Communication*, vol. 11 (2017): 1486-1506.

28 Bland dessa sektorer var: nästa generations it, maskindelar och robotik, nya material, och biomedicin, Tomoo Marukawa, ”The Evolution of China's Industrial Policy and 'Made in China 2025'”, i *Chinese Politics and Foreign Policy under Xi Jinping: The Future Political Trajectory*, red. Arthur S. Ding and Jagannath P. Panda (London och New York: Routledge, 2021), 131–49.

29 Fei Wu, m.fl., ”Towards a New Generation of Artificial Intelligence in China”, *Nature Machine Intelligence*, vol. 2, nr. 6 (2020): 312–16.

30 Se exempelvis Renai Jiang, Haoyue Shi och Gary H. Jefferson, ”Measuring China's International Technology Catchup”, *Journal of Contemporary* China, vol. 29, nr. 124 (2020): 519–34; Jolly, *The New Threat*, 20; Ana Maria Santacreu och Heting Zhu, ”What Does China's Rise in Patents Mean? A Look at Quality vs. Quantity”, *Economic Synopses*, nr. 14 (2018): 1–2.

31 Se Zeyi Yang, ”China Just Announced a New Social Credit Law. Here's What It Means”, *MIT Technology Review*, 22 november 2022; Lauren Yu-Hsin Lin och Curtis J. Milhaupt, ”China's Corporate Social Credit System: The Dawn of Surveillance State Capitalism?”, *The China Quarterly*, nr. 256 (2023): 835–53.

rekrytering av utländsk expertis och kunskapsinhämtning; samt att utländska företag har strategiskt förfördelats på den inhemska marknaden.[32]

## 6.3 Internet i dag i Kina

Enligt kinesiska statliga källor finns i dag 1 092 miljarder internetanvändare i Kina, vilket motsvarar 77,5 procent av befolkningen.[33] Samtidigt innebär det att över 300 miljoner invånare fortfarande saknar tillgång till internet. Dessutom finns stora skillnader i digital litteracitet mellan stad och landsbygd, vilka i sin tur förstärks av socioekonomiska och demografiska faktorer.[34]

Den genomsnittliga uppkopplade kinesen spenderar fem timmar och 33 minuter dagligen på internet.[35] I stort sett alla internetanvändare använder sociala medier och spenderar i snitt närmare två timmar om dagen på sex–sju olika plattformar, vilka i fallande procentuell användarordning är:

- WeChat med 87,3 procent av alla internetanvändare i Kina
- Douyin (78,4 procent)
- QQ (59,8 procent)
- Baidu Tieba (58,8 procent)
- Xiaohongshu (51,2 procent)
- Kuaishou (47,6 procent)
- Weibo (46,8 procent)

WeChat är en multifunktionell plattform, utvecklad av Tencent, som omfattar funktioner för sociala nätverk, e-handel, betalningar och andra tjänster. Douyin, utvecklat av ByteDance, är en videodelningsplattform vars motsvarighet i västländer är TikTok. QQ, utvecklad av Tencent, startade som en enkel chattklient men har med tiden blivit en mer avancerad plattform för sociala nätverk. Baidu Tieba, utvecklad av Baidu, är en diskussionsplattform där användare kan skapa och delta i ämnesbaserade forum. Xiaohongshu är en plattform för recensioner och e-handel, främst inriktad på skönhet, mode och livsstil som är utvecklad av Xingin. Kuaishou, utvecklad av Beijing Kuaishou Technology, är en videodelningsapp som liknar TikTok. Weibo, utvecklad av Sina Corporation, är en mikroblogg som liknar Twitter/X.

Den överlägset vanligaste enheten för internetåtkomst är mobiltelefonen, som används av 99,9 procent av Kinas uppkopplade befolkning. Inhemska varumärken (Vivo, Huawei, Oppo, Honor och Xiaomi) har tillsammans de största marknadsandelarna, medan Apple tidigare har legat i toppskiktet men just nu befinner sig bakom de kinesiska tillverkarna.[36] På marknaden för läsplattor dominerar Huawei och Apple med 26 procent var.[37] Beträffande operativsystem i mobila enheter använder runt 80 procent av konsumenterna Googles Android, följt av drygt 20 procent som föredrar Apples iOS. Samtidigt antar många bedömare att Huaweis relativt nya operativsystem HarmonyOS kommer ta en ökande andel av marknaden framöver.[38]

När det gäller bärbara och stationära datorer har användningen minskat, och ligger nu på omkring 30 procent vardera. Bland de största tillverkarna dominerar tre kinesiska bolag: Lenovo (34 procent), Huawei (13 procent) och TongFang (8 procent), samt amerikanska HP (9 procent) och taiwanesiska Asus (7 procent).[39] Redan 2001 började Kina att utveckla egna operativsystem (Kylin och NeoKylin) som enligt kinesiska källor används på 90 procent av statliga datorer.[40] Privata användare använder dock främst Apple OS och Microsoft Windows, men 2022 lanserades det Linuxbaserade openKylin, som i Kina marknadsförs

32 Se exempelvis Kerry Brown, *CEO, China: The Rise of Xi Jinping* (London och New York: I. B. Tauris, 2016); Sebastian Heilmann, *Red Swan: How Unorthodox Policymaking Facilitated China's Rise* (New York: Columbia University Press, 2018); Jin Hong, Song Hong, Liangbing Wang, Yi Xu och Dingtao Zhao, ”Government Grants, Private R&D Funding and Innovation Efficiency in Transition Economy”, *Technology Analysis & Strategic Management,* vol. 27, nr. 9 (2015): 1068–96; Rühlig, *The Sources of China's*.

33 Kinas informationscenter för internetnätverk, ”The 53rd Statistical Report on China's Internet Development”, mars 2024.

34 Anson Au, ”Digitalization in China: Who's Left behind?”, *Information, Communication & Society*, vol. 27, nr. 6 (2023): 1247–65.

35 Om inget annat anges hämtas statistiska data från: Simon Kemp, ”Digital 2024: China”, *DataReportal*.

36 International Data Corporation (IDC), ”Chinese Smartphone Market Accelerates to 8.9% Growth in 2Q24, Led by Chinese OEMs”, 26 juli 2024.

37 ”Different Fortunes in China as PC Shipments Fall 6% while Tablets Grow 20% in Q2 2024”, *Canalys*, 27 september 2024.

38 ”Chinese Operating Systems to See Explosive Growth as US Crackdown Speeds up Self-Reliance Process: Experts”, *Global Times*, 4 januari 2024; Lionel Lim, ”Huawei's Homegrown Operating System, Launched after the Company Was Put on a U.S. Blacklist, May Soon Overtake Apple's iOS in China”, *Fortune*, 4 januari 2024.

39 ”Different Fortunes”, *Canalys*.

40 Catalin Cimpanu, ”Two of China's largest tech firms are uniting to create a new 'domestic OS'”, *Zdnet/International*, 11 december 2019.

som ett helt inhemskt system avsett att konkurrera ut de amerikanska alternativen.[41] De vanligaste webbläsarna är Chrome (51,5 procent), Safari och Edge (båda 12,8 procent), medan den största sökmotorn är kinesiska Baidu (66,3 procent).

Ur användarperspektiv förefaller styrets satsningar på inhemsk utveckling ha burit frukt, inte minst genom att kinesiskt tillverkade produkter ökat i popularitet. Samtidigt som beroendet av amerikansk teknik och mjukvara har minskat är det dock fortfarande betydande.[42] I fråga om världens största teknikbolag sett till omsättning rankas Huawei och Tencent på sjunde respektive tionde plats globalt.[43] Tre av de tio största telekomföretagen är kinesiska: China Mobile Communications (1:a), China Telecommunications (7:e) och China United Network Communications (9:e).[44] Inom e-handel är Alibaba världens sjätte största återförsäljare.[45]

I dagsläget är Kina kopplat till 13 undervattenskablar, varav åtta går till asiatiska länder, tre till USA och en till Europa och en till Afrika.[46] Kina har dock bara tre internetknutpunkter för anslutning till det globala internet, så kallade *Internet Exchange Points* (IXP:er), belägna i Peking, Shanghai och Guangzhou. Detta möjliggör större kontroll över dataflöden och en teoretisk möjlighet att stänga av Kina från det globala internet.[47] Få IXP:er leder dock till flaskhalsar och som svar på detta lanserades 2023 det omfattande infrastrukturprojektet ”Framtida internet-teknikinfrastruktur”, som enligt kinesiska medier ska ge höghastighetsinternet över hela landet med hastigheter på upp till 1,2 Tb/s.[48]

Utöver detta har Kina i dag världens största nätverk av basstationer för femte generationens (5G) internet med en relativt god bredd av frekvenser för 5G, med lågfrekvensband för landsbygden (god täckning men långsammare hastighet), en omfattande utbyggnad av mellanfrekvensband i tätorter (bra balans mellan räckvidd och hastighet), samt planer på att använda högfrekvensband för tätbefolkade urbana miljöer och i industrin (mycket snabb hastighet men sämre täckning).[49] Kinas omfattande användning av mellanfrekvensband för 5G, kan stärka Kinas industriella konkurrenskraft inom sektorer där snabb och stabil kommunikation är avgörande för industriell implementering av sakernas internet (*Internet of Things*) och annan avancerad tillverkning.[50]

Offentliga siffror om antalet datacenter i Kina varierar mellan 250 och 400. Med stor sannolikhet finns även hemliga datacenter. Sammantaget handlar det om hundratals miljoner servrar,[51] vilket enligt kinesiska uppgifter placerar landet på andra plats globalt när det gäller datorkraft. Traditionellt har kinesiska företag dominerat sektorn, men ett nytt pilotprogram tillåter utländskt ägande av datacenter och informationsteknik i vissa regioner, vilket öppnar för internationella aktörer. I kinesiska medier anges anledningen vara att öka förmågan för hantering av stora datamängder och främja användande av artificiell intelligens (AI), samt att skapa kinesiska produkter för den internationella marknaden.[52]

I den 14:e femårsplanen (2021–2025) betonade Kommunistpartiet behovet av ökad självförsörjning i strategiska tekniker, såsom sakernas internet, AI, halvledare, kvantberäkning, 5G, bioteknik och nya material.[53] Digitalisering förväntades dessutom få en än större roll i samhället, staten och ekonomin. Dessa mål underströks även under Kommunistpartiets 20:e partikongress 2022,

41 ”China’s first Root-Community of Desktop Operating System, OpenKylin, Makes Debut”, *Global Times*, 30 juni 2022; Liam Proven, ”China’s openKylin 1.0 arrives. Our verdict? Not a bad-looking, er, Ubuntu remix”, *The Register*, 7 juli 2023.

42 Pengfei Han, Wei Jiang och Danqing Mei, ”Mapping U.S.–China Technology Decoupling: Policies, Innovation, and Firm Performance”, *Management Science,* vol. 70, nr. 12 (2024): 8386–8413.

43 ”Fortune Global 500: Technology”, *Fortune*, 3 oktober 2024.

44 ”Fortune Global 500: Telecommunications”, *Fortune*, 3 oktober 2024.

45 ”Fortune Global 500: Information Technology Services”, *Fortune*, 3 oktober 2024.

46 Hong Kong är ej inräknat. Se Submarine Cable Networks, ”China”, 9 januari 2025.

47 Cheng, *Cyber Dragon*, 67.

48 ”World’s First 1.2TB Ultra-High-Speed Backbone Network Ppens in China”, *Global Times*, 13 november 2023.

49 Det handlar i synnerhet om frekvenserna n41 (2,515–2,675 GHz), n78 (3,4–3,6 GHz) och n79 (4,8–4,9 GHz) samt planer att använda n258 (24,75–27,5 GHz).

50 ITU-R, *IMT Vision – Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond*, M.2083-0, M Series, Geneve, 2015.

51 Mer specifikt rör det 7,5 miljoner så kallade standardrack. Ett standardrack är ett slags bokhylleställ för servrar och ett rack är ungefär två meter högt och kan rymma många servrar. 7,5 miljoner rack motsvarar hundratals miljoner servrar och innebär en enorm datakapacitet, Daniel Slotta, ”Cumulative Size of Chinese Data Centers from 2019 to August 2023”, *Statista*, 5 juli 2024.

52 Tu Lei, ”China Prepares to Pilot Opening-Up of Internet Data Centers: Minister”, *Global Times*, 8 mars 2024.

53 Asiatiska utvecklingsbanken, ”The 14th Five-Year Plan of the People’s Republic of China – Fostering High-Quality Development”, 2021; Nis Grünberg, ”China’s 14th Five-Year Plan – Strengthening the Domestic Base to Become a Superpower”, *MERICS*, 9 april 2021.

då Kina uttalade sin avsikt att bli ett av världens mest innovativa länder.[54]

Landets tekniska och teknologiska framsteg sedan 1980-talet är tydliga med en stark internetsektor en ekonomi som har vuxit explosionsartat. Produktion per person har ökat med omkring 3 000 procent och den ekonomiska tillväxten mätt i bruttonationalprodukten har legat kring 8–9 procent per år sedan 1980.[55] Därtill har Kina en ledande position inom utvinning och export av sällsynta jordartsmetaller, vilka är av avgörande betydelse för både grön omställning och avancerad teknik.[56]

Trots att Kina har nått långt återstår en rad hinder. Landet rankades exempelvis på 19:e plats 2023 i det globala digitala världskonkurrenskraftsindexet, långt efter USA (1:a), Sverige (7:e) och Israel (13:e).[57] I fråga om molntjänster, en av de strategiska marknaderna som Kommunistpartiet vill dominera, står kinesiska bolag för en blygsam andel på sex procent, medan amerikanska företag har största andelen av marknaden med cirka 70 procent.[58] Vad gäller operativsystem för datorer är kinesiska alternativ än så länge obetydliga i global jämförelse med de amerikanska dominerande aktörerna.[59]

I Kina sker en idag en rad AI-satsningar. Peking har nyligen lanserat initiativet ”AI-plus”, Baidu liksom Alibaba har introducerat avancerade AI-modeller (Ernie LLM respektive Qwen) och flera nya bolag, kallade ”AI-tigrar” (bland andra Baichuan, DeepSeek, Moonshot AI, Minimax och Zhipu), gör stora framsteg inom AI-utveckling. Detta till trots ligger landet fortfarande efter USA och EU.[60] USA har 61 etablerade AI-modeller mot Kinas 15 och investerar närmare nio gånger mer i forskning och utveckling. Amerikanska universitet och företag rankas också högre vad gäller forskning kring AI.[61] Utvecklingen är dock mycket snabb inom detta fält och i början av 2025 hävdade både ByteDance och DeepSeek att deras AI-modeller presterade bättre än de ledande amerikanska modellerna.[62]

Tillväxten i Kina förväntas avta och enligt Internationella valutafonden kan den hamna kring tre procent vid slutet av detta decennium.[63] Dessutom skapar det globala säkerhetspolitiska läget en viss osäkerhet kring Kinas fortsatta expansion, inte minst när det gäller it-infrastruktur och digitala produkter.[64] En växande protektionism och en mer omfattande säkerhetspolitisk inramning av marknaderna i både Kina och utlandet påverkar potentialen för samarbete över gränserna.[65] Exempelvis har Kommunistpartiets underrättelselag från 2017, som ålägger alla kinesiska aktörer att på begäran samarbeta med den kinesiska underrättelseapparaten, fått aktörer i väst att bli mer återhållsamma i samarbeten med kinesiska bolag.[66] Därtill har kontraspionagelagen från 2023 breddat definitionen av vad som räknas som säkerhetskänslig data, något som ytterligare kan dämpa de internationella affärskontakterna för kinesiska företag.[67]

Sammantaget har Kina gjort iögonfallande framsteg på cyberområdet med betoning på ökad självförsörjning och fortsatta innovationer i de fysiska och logiska lagren. Landet är i vissa avseenden en världsledande cybernation, med starka inhemska bolag och höga ambitioner i såväl digital som industriell utveckling. Vidare har utvecklingen resulterat i att Kina till stor del är självförsörjande inom tekniksektorn och sannolikt skulle klara sig bra vid oroligheter i globala leverantörskedjor och vid säkerhetspolitisk instabilitet. Trots detta återstår en komplicerad balansgång mellan ekonomisk tillväxt, teknisk självförsörjning, internationell konkurrenskraft och ett omvärldsläge där säkerhetspolitiska faktorer kan bromsa Kinas fortsatta expansion. Styret i Kina har därmed att hantera både en framgångsrik inhemsk utveckling och de hinder som följer av ökad global skepsis och

54 För en analys av den 20:e partikongressen, se: Patrik Andersson, m.fl., ”Kommunistpartiets 20:e nationella kongress: Xi Jinping stärker sitt grepp om Kina”, Brief nr. 4 (Stockholm: Nationellt kunskapsscentrum om Kina, 2022).

55 Spencer Feingold, ”Where is China’s Economy Headed?”, *World Economic Forum*, 27 juni 2024.

56 Som kritiska mineraler räknas: aluminium, kobolt, koppar, litium, mangan, nickel, naturlig grafit och andra sällsynta jordartsmetaller. Se FN:s konferens om handel och utveckling, ”Digital Economy Report 2024: Shaping an Environmentally Sustainable and Inclusive Digital Future”, Förenta nationerna, 11 juli 2024.

57 International Institute for Management Development, ”World Digital Competitiveness Ranking 2023”.

58 Statistiken refererar till Q1 2024, Felix Richter, ”Amazon Maintains Cloud Lead as Microsoft Edges Closer”, *Statista*, 2 maj 2024.

59 Statcounter Globalstats, ”Operating System Market Share Worldwide Sept 2023 – Sept 2024”.

60 Drew Bernstein, ”Who Is Winning the AI Arms Race?”, *Forbes*, 28 augusti 2024.

61 Ray Perrault och Jack Clark, *Artificial Intelligence Index Report 2024* (Stanford: Stanford University Human-Centered Artifical Intelligence (HAI), 2024), 19.

62 Liam Mo och Brenda Goh, ”TikTok Owner ByteDance, DeepSeek Lead Chinese Push in AI Reasoning”, *Reuters*, 22 januari 2025.

63 Feingold, ”Where is China’s”.

64 För en mer detaljerad diskussion, se Rühlig, *The Sources of China’s*.

65 Ryan Woo, ”China Wants to Mobilise Entire Nation in Counter-Espionage”, *Reuters*, 2 augusti 2023.

66 Jill Goldenziel, ”China’s Anti-Espionage Law Raises Foreign Business Risk”, *Forbes*, 3 juli 2023.

67 Woo, ”China Wants to Mobilise”.

växande protektionistiska tendenser. Det slutliga utfallet i förhandlingarna om handelstullar mellan Kina och USA kommer att få stor betydelse.

## 6.4 Kina, säkerhetspolitik och Brics

Kinas syn på internet, cyber och säkerhetspolitik är tätt sammanlänkad med landets ambition att både värna nationell suveränitet och stärka sin globala ställning. Ett säkerhetspolitiskt uppvaknande skedde 2013 när Edward Snowden avslöjade USA:s underrättelsearbete mot bland annat Huawei, vilket uppfattades som ett hot mot kinesisk säkerhet.[68] Därtill har demokratiska gräsrotsrörelser som varit delvis organiserade via internet, som färgrevolutionerna i före detta sovjetrepubliker, den arabiska våren och protesterna i Hongkong, övertygat Kommunistpartiet om att kontroll över internet är avgörande för att upprätthålla inhemsk stabilitet.[69]

I ett uttalande 2014 framhöll Xi Jinping att ”utan cybersäkerhet finns det ingen nationell säkerhet”.[70] Vid en konferens för cybersäkerhet 2016 gick han längre och menade att ”stormakternas kamp om cybersäkerhet inte bara handlar om teknik, utan också om makten över idéer och samtalet”.[71] Det här uttalandena illustrerar hur politiska system och informationsteknik är sammanflätade där de tillsammans blir en fråga för regimsäkerhet. Å ena sidan talas det om cybersäkerhet (säkra system och nätverk), å den andra om innehållskontroll (vilka idéer som får cirkulera på internet). De knyter vidare an till utrikespolitiska motsättningar mellan Kina (liksom Ryssland) och väst, som har präglat förståelsen av vad ett säkert internet innebär (för vidare diskussion, se slutsatserna i kapitel 8).

Denna inställning har lett till att forskning och nyhetsmedier ofta talar om ett ”kallt teknikkrig” mellan Kina och USA.[72] Oavsett vilka liknelser som föredras är det tydligt att kontrollen över det fysiska och det logiska lagret har blivit centrala komponenter i Kinas relation till omvärlden. Ur kinesiskt perspektiv handlar detta om att skydda sig mot ett aggressivt USA och västligt ideologiskt inflytande, där den amerikanska exportkontrollen som infördes mot Kina 2022 anses visa på vikten av att bli tekniskt oberoende på cyberområdet.[73]

### Kinas cyberpolitik och internationell säkerhet

Det kinesiska ledarskapet har länge förstått samspelet mellan politik, teknologi och teknisk standardisering. Denna holistiska syn kan delas upp i tre perspektiv: (1) nationell suveränitet, (2) informationskontroll och (3) standardisering.[74] Dessa perspektiv genomsyrar Kinas säkerhetspolitiska hållning och påverkar även hur landet agerar i internationella sammanhang.

Det första perspektivet handlar om cybersuveränitet. I ett tal 2015 klargjorde Xi suveränitetens kärna: 1) att respektera varje lands rätt att själv bestämma sin väg för internetutveckling, välja sin egen modell för internetstyrning och utforma egna offentliga regler för internetanvändning; samt (2) att delta jämlikt i det internationella samarbetet kring cybersäkerhet, där stater bör undvika så kallade cyberhegemonier och avstå från att blanda sig i andra länders interna angelägenheter, vilket var en indirekt hänvisning till USA:s och andra västländers tidigare ageranden.[75] Trots att Xi i internationella sammanhang talar om vikten att undvika cyberhegemonier har han sedan 2012 deklarerat att Kina ska bli en ”cyberstormakt”,[76] vilket enligt Xi är en viktig pusselbit i att realisera hans politiska vision ”den kinesiska drömmen”.[77]

Som ett led i denna utveckling presenterade Kinas cyberrymdadministration landets första cybersäkerhetsstrategi 2016. Här beskrivs hur kritisk infrastruktur

68 Creemers, ”The Chinese Conception”, 182; Cheung, ”The Rise of China”, 310–11.

69 Cheng, *Cyber Dragon*, 73; Qiao-Franco, ”An Emergent Community”, 5.

70 Doshi, m.fl., *China as a ”Cyber Great Power”,* 9.

71 Citerad och översatt från engelska i Doshi, m.fl., *China as a ”Cyber Great Power”*, 9.

72 Gregory C. Allen, ”China Is Striking Back in the Tech War With the U.S”, *TIME*, 20 juli 2023; Creemers, ”The Chinese Conception”; Caitlin Lee, ”Winning the Cold Tech War”, Rand, Santa Monica, 17 augusti 2023; Adam Segal, ”The Coming Tech Cold War With China Beijing Is Already Countering Washington’s Policy”, *Foreign Affairs*, 9 september 2020.

73 Gregocy C. Allen, *China’s New Strategy for Waging the Microship War* (Washington D.C.: Center of Strategic & International Studies, 2023); Tao Mingyang, ”China’s Homegrown Operating System Sees Rapid Development as US’ Tech Assault Backfires”, *Global Times*, 10 augusti 2023.

74 Stacie Hoffmann, Dominique Lazanski och Emily Taylor, ”Standardising the Splinternet: How China’s Technical Standards Could Fragment the Internet”, *Journal of Cyber Policy*, vol. 5, nr. 2 (2020): 239–64, 242.

75 Cheung, ”The Rise of China”, 312.

76 Creemers, ”The Chinese Conception”, 173.

77 Det handlar om ett framtida Kina som är 1) ekonomiskt, politiskt, vetenskapligt och militärt starkt, 2) civiliserat, kulturellt och moraliskt 3) harmoniskt och klassöverbryggande, samt 4) ekologiskt hållbart, grönt och vackert. Se Lidya Christin Sinaga, ”Xi Jinping, ‘China Dream’, and Chinese Military Diplomacy to ASEAN”, *JAS (Journal of ASEAN Studies)*, vol. 8, nr. 2 (2021): 173–90, 174.

måste säkras och hur staten har rätt att kontrollera internet.[78] I planen lyfts särskilt hot mot ekonomisk, politisk, kulturell och social säkerhet, där digitalisering anses göra Kina sårbart för cyberattacker och utländsk påverkan.[79] Den röda tråden är att cybersäkerhet och säkerhetspolitik smälter ihop, och att Kina beskrivs behöva öka sin förmåga till både cyberavskräckning och som ett led i det,[80] militär-civil integration för förmågeutveckling.[81] Vid sidan av civila myndigheter har Kina därför satsat på att utbilda nya experter och inrätta cyberinstitutioner (exempelvis det Nationella cybersäkerhetscentret i Wuhan) för att främja innovation och förmågetutveckling.[82]

I Belfercentrets index för cyberförmågor från 2022 rankas Kina som tvåa efter USA med världsledande offensiva förmågor och en stark ekonomi kring övervakning, information och underrättelseinhämtning.[83] I en rapport från 2025 noterar det amerikanska cybersäkerhetsföretaget Palo Alto Networks att Kinas offensiva förmågor blir alltmer sofistikerade samt att de används likväl mot Kinas strategiska konkurrenter som mot allierade.[84] Kinas defensiva förmågor rankas dock lågt. En tolkning är att Kinas starka fokus på informationskontroll – och restriktioner mot krypterad trafik – skapar sårbarheter, eftersom resurser läggs på övervakning av innehåll på internet snarare än på att säkra själva systemen.[85]

Det andra perspektivet i Kinas säkerhetspolitik rör just informationskontroll. Redan 2014 varnade Xi partikadrer för att kritiska röster och negativa uppfattningar skulle kunna underminera hans vision om den ”kinesiska drömmen” och talade explicit om ”Tacitus fälla”, dvs. att en ledare som förlorat sin popularitet misstänks för dåliga avsikter oavsett hur denne agerar. I forskning beskrivs detta som Kommunistpartiets ”största rädsla”, vilket driver partiet att ständigt övervaka och styra det offentliga samtalet, både hemma och utomlands.[86]

Informationskontroll är inget nytt i Kina, men metoderna har förfinats.[87] I stället för tidigare öppen repression talas det nu om ”harmoni”, ”respekt” och ”framgång” samtidigt som partistaten använder avancerad PR, opinionsundersökningar och digital masspåverkan.[88] Systemet är dock inte helt monolitiskt utan rymmer nyanser.[89] Grundregeln är ändå att allt som riskerar social och politisk mobilisering ska stoppas.[90]

Den så kallade Gyllene skölden (internationellt känd som *The Great Firewall of China*) är Kinas främsta verktyg för internetcensur.[91] Lanserad redan 1996 men fullt implementerad först 2008, blockerar, filtrerar och begränsar den trafik till och från globala nätverk.[92] Därtill stryps ibland bandbredd till vissa tjänster, så att användare frivilligt slutar besöka dem. Andra exempel på metoder är att begränsa internetanvändares möjlighet att koppla upp sig mot det globala internet och använda utländska kommunikationsplattformar, att blockera webbsidor, försvåra användandet av krypterad trafik, begränsa sökmotorers resultat samt genom innehålls-modifiering och moderering.[93] Målet är att

78 Creemers, ”The Chinese Conception”, 183.
79 Cheung, ”The Rise of China”, 312.
80 Cheung, ”The Rise of China”, 317.
81 Doshi, m.fl., *China as a ”Cyber Great Power”*, 4.
82 Dakota Cary, ”China’s National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain”, Issue Brief (Washington D.C.: Center for Security and Emerging Technology (CSET), 2021), 7.
83 Julia Voo, Irfan Hemani och Daniel Cassidy, ”National Cyber Power Index 2022” (Cambridge, MA: Belfer Center, 2022), 10–12.
84 Dena De Angelo, ”Global Reach – The New Scale of Chinese Cyberthreats”, Palo Alto Networks, 26 juni 2025.
85 Se Valentin Weber, ”How China’s Control of Information is a Cyber Weakness”, *Lawfare*, 12 november 2020.
86 Jesse S. Curtis, ”Springing the ‘Tacitus Trap’: Countering Chinese State-Sponsored Disinformation”, *Small Wars & Insurgencies*, vol. 32, nr. 2 (2021): 229–65, 230.
87 Maria Repnikova och Kecheng Fang, ”Authoritarian Participatory Persuasion 2.0: Netizens as Thought Work Collaborators in China”, *Journal of Contemporary China*, vol. 27, nr. 113 (2018): 763–79, 763.
88 Anne-Marie Brady och Wang Juntao, ”China’s Strengthened New Order and the Role of Propaganda”, *Journal of Contemporary China*, vol. 18, nr. 62 (2009): 767–88, 786.
89 Se vidare Ruichen Zhang, ”Negotiating Censorship through ‘Socialist Recoding’ on the Chinese Internet: Nuances and Potentialities in a Contested Cyberspace”, *Information, Communication & Society*, vol. 27, nr. 1 (2024): 126–42, 127.
90 James Griffith, *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet* (London och New York: Zed Books, 2021), 9.
91 Sonali Chandel, et al, ”The Golden Shield Project of China: A Decade Later—An in-Depth Study of the Great Firewall”, *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)* (2019): 111–19, 111.
92 Guanying Li, ”Internet Censorship in China: A Functioning Digital Panopticon”, i *Communications in Contemporary China: Orchestrating Thinking*, red. Nicole Talmacs och Altman Yuzhu Peng (Abingdon och New York, 2024), 11–26, 14. Se även: Luzhou Li och Kui Zhou, ”When Content Moderation Is Not about Content: How Chinese Social Media Platforms Moderate Content and Why It Matters”, *New Media & Society*, online first (2024): 1–17; Mingshi Wu, m.fl., ”How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic”, *32nd USENIX Security Symposium* (2023): 2653–70.
93 Cheng, *Cyber Dragon*, 67.

censuren ska bli så pass omärkbar att medborgarna inte protesterar mot den.

Utöver detta använder statsapparaten ett omfattande nät av lagar och regleringar, administrerade av över 70 statliga institutioner.[94] Ofta är lagarna breda och tolkningsutrymmet stort, vilket leder till självcensur bland företag och enskilda.[95] Forskare beskriver denna kombination av övervakningsteknik, infrastrukturkontroll och självreglering som ”världens mest sofistikerade regim för internetkontroll”.[96] Samtidigt är det tydligt att syftet går långt bortom ren säkerhet – det handlar om att säkra partiets legitimitet och politiska monopol. I Freedom House index över frihet på internet rankas Kina tillsammans med Myanmar som sämst i världen.[97]

Det tredje perspektivet rör Kinas strävan att påverka internets grundläggande arkitektur via internationell standardisering. Internet och modern informationsteknik vilar på olika standarder (t.ex. Wi-Fi, IP-adresser, USB, HTML) som tagits fram inom ett brokigt system av standardutvecklande organisationer (SDO:er), såsom *Internet Corporation for Assigned Number and Names* och FN-organet Internationella teleunionen (ITU) (se kapitel 2). Historiskt har amerikanska och europeiska aktörer dominerat dessa processer, men Kina har sedan 2006–2007 aktivt deltagit för att få sina egna nationella standarder accepterade internationellt.[98]

Ett konkret exempel är förslaget om ”Nytt IP”, framlagt av Huawei till ITU 2019, där syftet var att ändra internets grundläggande protokoll (TCP/IP).[99] Förslaget avfärdades, men arbetet fortsätter i Kina. Kritiker menar att ”Nytt IP” skulle kunna öka fragmenteringen av internet, eftersom det riskerar att skapa nya, mer kontrollerade nationella eller regionala intranät. Kinesisk teknik för övervakning och dataanalys skulle därtill kunna byggas in i själva arkitekturen.[100]

Kinas modell för standardisering är i grunden statsdriven och bygger på ett multilateralt styre av internet, dvs. att regeringar förhandlar med regeringar snarare än flerpartslösningar som hittills har präglat internets styrning och reglering.[101] Landet har ökat sin representation i olika SDO:er samt uppmuntrat inhemska företag som Huawei och Tencent att inta en mer framträdande roll. Kina har även haft generalsekreterare i Internationella standardiseringsorganisationen och ITU.[102] Genom lagar som Standardiseringslagen (2018) och programmet ”Kinastandarder 2035” betonas vikten av forskning, industriellt samarbete och ökat globalt inflytande.[103] Samtidigt talar Kina gärna om ”öppenhet” och ”rättvis konkurrens” på den internationella arenan, vilket i sig inte är särskilt anmärkningsvärt givet USA:s dominans, medan inrikesretoriken slår fast vikten av att inte bli beroende av utländsk teknik.[104]

## Kinas cyberpolitik och Brics

Som har diskuterats i kapitlets inledande del är Brics en viktig arena för Kinas säkerhetspoliska arbete, vilket även är tydligt i relation till cyberområdet. Under 2014 års Bricsmöte i Fortaleza, Brasilien, underströk Xi exempelvis att Brics-länderna skulle arbeta för ”världsfred

94 Li, ”Internet Censorship in China”, 12.

95 Li, ”Internet Censorship in China”, 12; Milton L. Mueller, ”China and Global Internet Governance: A Tiger by the Tail”, i *Access Contested: Security, Identity and Resistance in Asian Cyberspace*, red. Ronald Deibert, John Palfrey, Rafal Rohozinski och Jonathan Zittrain (Cambridge: MIT Press, 2011): 177–94, 181.

96 Alex Mueller och Christopher S. Yoo, ”Crouching Tiger, Hidden Agenda?: The Emergence of China in the Global Internet Standard-Setting Arena”, *Federal Communications Law Journal*, vol. 76, nr. 23–33 (2024): 143: 1–71, 38.

97 Freedom House, ”Freedom on the Net 2024: The Struggle for Trust Online” (Washington, DC: Freedom House, 2024), 25.

98 Courtney J. Fung, ”China’s Use of Rhetorical Adaptation in Development of a Global Cyber Order: A Case Study of the Norm of the Protection of the Public Core of the Internet”, *Journal of Cyber Policy*, vol. 7, nr. 3 (2022): 256–274.

99 Campanella och Haigh, ”The Battle for the Internet”, 76.

100 Hoffmann, m.fl., ”Standardising the Splinternet”, 244.

101 Tim Nicholas Rühlig, *Technical Standardisation, China and the Future International Order* (Bryssel: Heinrich Böll Stiftung, 2020).

102 Edoardo Campanella och John Haigh, ”The Battle for the Internet”, *Survival*, vol. 66, nr. 1 (2024): 69–84, 73; Hoffmann, m.fl., ”Standardising the Splinternet”, 243; Se vidare: Gianlugi Negro, ”The Rising Role of China in the Promotion of Multilateral Internet Governance, 1994–2014”, i *History of the International Telecommunication Union (ITU): Transnational Techno-Diplomacy from the Telegraph to the Internet*, red. Gabriele Balbi och Andreas Fickers (Oldenbourg: De Gruyter, 2020): 107–134; Lennart Schott och Kerstin J. Schaefer, ”Acceptance of Chinese Latecomers’ Technological Contributions in International ICT Standardization — The Role of Origin, Experience and Collaboration”, *Research Policy*, vol. 52, nr. 1 (2023): artikel nr. 104656, 1–16.

103 Center for Security and Emerging Technoogy (CSET), ”The Central Committee of the Communist Party of China and the State Council issued the National Standardization Development Outline”, *Xinuha News Agency*, 10 oktober 2021; Hoffmann, m.fl., ”Standardising the Splinternet”, 247.

104 Doshi, m.fl., *China as a ”Cyber Great Power”*.

och stabilitet" där cybersäkerhet var ett "nyckelområde" för samarbete.[105]

Utöver säkerhetspolitiska deklarationer är det tydligt att Kina har tagit en ledande roll inom teknologi och teknikutveckling i Brics. År 2017 samlades femtio delegater från Bricsländerna i Kunming för det första dedikerade mötet i ämnet (*BRICS Technology Transfer Cooperation Forum and Workshop*). Där lanserades en handlingsplan för tekniköverföring,[106] inklusive etableringen av ett tekniköverföringscentrum i Kunming, som formellt upprättades 2018.[107] År 2022 hölls det första mötet för centrumets styrkommitté, där representanter från medlemsländernas myndigheter för vetenskap, teknik och innovation deltog, tillsammans med experter och tekniköverföringsorganisationer.[108]

Ett annat Kina-lett initiativ är Brics-institutet för framtida nätverk, lanserat 2019 i Shenzhen (ofta kallat för Kinas Silicon Valley).[109] Institutet samarbetar kring forskning, standardisering och teknikutveckling genom gemensamma projekt och utbyten av expertis. Fokus ligger på framtidens nätverk, ny teknik och innovation, med målet att driva både privat och statlig forskning och utveckling samt bidra till internationella standarder.[110]

Under Brics-toppmötet i oktober 2024 betonade Xi Jinping vikten av innovation och högkvalitativ utveckling samt underströk Kinas vilja att fördjupa samarbetet för en gemensam framtid präglad av utveckling och framsteg. Han uppmanade Brics-länderna att "agera pionjärer" och hålla jämna steg med den pågående tekniska revolutionen och industriella omvandlingen.[111] Som en del av denna vision framhöll Xi det nyligen etablerade och Kinaledda Bricscentrumet för AI och andra initiativ för stärkt samarbete inom innovation och teknik, bland annat genom Brics internationella forskningscenter för djuphavsresurser.[112]

Även om Peking använder Brics för att stärka sitt internationella inflytande och främja standardisering av internet och it-infrastruktur, finns det i den undersökta litteraturen få bevis för att partiet försöker skapa ett separat Brics-internet. En annan viktig aspekt är dock Kinas "Digitala sidenväg", en del av det större Sidenvägsinitiativet (*Belt & Road Initiative*).[113] Huvudmålen är att utöka kinesiskägd infrastruktur för finans, e-handel och molntjänster. Det innefattar projekt som undervattenskablar, samarbete kring smarta städer och e-handelsförbindelser. Till det läggs diplomatiska insatser som fokuserar på att öka Kinas normativa inflytande över cybersäkerhetsstyrning och dataskyddsregler.[114] I vissa uttalanden från Peking framstår dock Sidenvägen som mer prioriterad än Brics.[115] Exempelvis framhöll Xi i ett tal 2017 att Brics "Nya utvecklingsbank och andra multilaterala utvecklingsinstitutioner" var verktyg för att stödja "Sidenvägsrelaterade projekt".[116]

Det framstår alltså som att Kina försöker koppla ihop sina olika multilaterala projekt för att stärka sin position globalt. Länder som Brasilien, Ryssland och Sydafrika kan lockas av kinesiska satsningar när det gäller infrastruktur och digital utveckling, särskilt om de upplever att västvärlden inte erbjuder motsvarande stöd. På så sätt kan Brics fungera som ytterligare språngbräda för Peking att befästa sitt ledarskap i frågor kring digital teknik, standarder och säkerhetsnormer.

## 6.5 Slutsatser

Kina har under Xi Jinping dragit upp tydliga linjer för hur cyberområdet ska hanteras ur säkerhetspolitiskt perspektiv i både det fysiska och det logiska lagret. Peking vill skydda landet mot yttre och inre hot,

105 Xinhua News Agency, "Xi Proposes Closer, More Solid BRICS Partnership", *China Daily*, 16 juli 2014.

106 "BRICS Technology Transfer Cooperation Mechanism formalised in Kunming, China", University of Cape Town, 9 januari 2018.

107 Brics ministermöte för vetenskap, teknik och innovation (STI), "Durban Declaration", 3 juli 2018.

108 Ministeriet för vetenskap och teknik, "China Participates in the First Meeting of the Steering Committee of BRICS Technology Transfer Center Network", Folkrepubliken Kina, 22 juni 2022.

109 "BRICS Set up new Institutional Branch to Strengthen Cooperation on ICT", *Xinhua*, 7 augusti 2019.

110 Brics institut för framtida nätverk (BIFN), "About BIFN".

111 Xi Jinping, "Embracing a Broader View and Cutting Through the Fog of Challenges to Advance High-Quality Development of Greater BRICS Cooperation", Utrikesdepartementet, Folkrepubliken Kina, 24 oktober 2024.

112 I officiella kommunikéer framhålls att centret ska samla Brics-ländernas främsta forskningskompetens inom djuphavsmineraler, energi, miljöstyrning och teknik, med fokus på djuphavsteknik och hållbar utveckling. Se: "BRICS deep-sea resources research center launched in Hangzhou", Kommunstyrelsen i Hangzhou, 27 april 2025.

113 Weifeng Zhou och Mario Esteban, "Beyond Balancing: China's Approach towards the Belt and Road Initiative", *Journal of Contemporary China*, vol. 27, nr. 112 (2018): 487–501.

114 Jing Cheng och Jinghan Zeng, "'Digital Silk Road' as a Slogan Instead of a Grand Strategy", *Journal of Contemporary China*, vol. 33, nr. 149 (2024): 823–38; Ying Huang och Maximilian Mayer, "Power in the Age of Datafication: Exploring China's Global Data Power", *Journal of Chinese Political Science*, vol. 28, nr. 1 (2023): 25–49.

115 Se vidare: Hooijmaaijers, "China, the BRICS", 41.

116 Xi Jinping, "Full text of President Xi's speech at the Opening of Belt and Road Forum", *Belt and Road Forum for International Cooperation*, 14 maj 2017.

kontrollera informationsflöden och utforma globala standarder. Samtidigt är Kinas hållning mer nyanserad än bara renodlad isolering där det står klart att global handel, innovation och standarder kräver interaktion med omvärlden. Brics-samarbetet illustrerar denna dubbelhet. Det är en plattform för att stärka Kinas globala inflytande och ledarskap på cyberområdet, men det är också ett pragmatiskt forum för att knyta ekonomiska och diplomatiska band. Vidare visar Kina att omfattande inhemsk kontroll kan samexistera med det globala internet.

I slutändan visar Kinas agerande i cyberfrågor hur säkerhetspolitik, inrikes kontroll och global maktutövning alltmer flätas samman, precis som kinesiska talespersoner själva ger uttryck för. I dag syns konturerna av en framtid där forskning och utveckling och teknikstandarder inte bara är tekniska utan också politiska – och där inflytande över internetarkitekturen blir en fråga om geopolitisk makt. Brics är en av flera arenor där Kina fortsätter att främja sina visioner för ett internationellt system som i högre grad speglar dess egna prioriteringar. Hur denna process utvecklas kan i förlängningen avgöra om internet fortsätter vara någorlunda globalt och öppet, eller om det splittras i flera delar med olika regler, normer och värderingar. Mot denna bakgrund förefaller Kinas satsningar och utveckling inom cyber och generell teknikutveckling drivas en dubbel ambition – att minska sårbarheten mot yttre ovälkommet inflytande samt att ta över den amerikanska globala dominansen på områdena.

Relationen till USA och utvecklingen av det så kallade kalla teknikkriget kommer att prägla hur ländernas rivalitet utformas,[117] vilket sannolikt kommer att inverka på omvärldens utveckling på cyberområdet, inte minst inom Brics. USA:s sanktioner mot Kina gör det svårt, för att inte säga omöjligt för Kina, att bli en ledande och självständig aktör i tillverkningen av de så viktiga halvledarna. Samtidigt förefaller detta stärka Pekings övertygelse om att bli självförsörjande i alla de tekniska lagren. Framtida ökade säkerhetspoliska spänningar mellan Kina och USA gör att en utveckling mot separata, eller avsevärt avskurna, tekniska och teknologiska ekosystem inte kan uteslutas.

117 För en omfattande analys av relationen mellan Kina och USA, se Johan Englund och Oscar Almén, *Den hundraåriga folkrepubliken: En bedömning av Kinas utveckling och relation till USA mot 2050*, FOI-R--5631--SE (Stockholm: Totalförsvarets forskningsinstitut, 2024).

# Referenser

”BRICS deep-sea resources research center launched in Hangzhou”. Kommunstyrelsen i Hangzhou, 27 april 2025, hämtad 10 september 2025, *https://www.ehangzhou.gov.cn/2025-04/27/c_293458.htm*.

”BRICS Set up new Institutional Branch to Strengthen Cooperation on ICT”. Xinhua, 7 augusti 2019, hämtad 15 november 2024, *http://www.xinhuanet.com/english/2019-08/07/c_138289903.htm*.

”BRICS Technology Transfer Cooperation Mechanism formalised in Kunming, China”. University of Cape Town, 9 januari 2018, hämtad 2 november 2024, *https://uct.ac.za/rci/articles/2018-01-09-brics-technology-transfer-cooperation-mechanism-formalised-kunming-china*.

”China’s first Root-Community of Desktop Operating System, OpenKylin, Makes Debut”. Global Times, 30 juni 2022, hämtad 12 november 2024, *https://www.globaltimes.cn/page/202206/1269494.shtml*.

”Chinese Operating Systems to See Explosive Growth as US Crackdown Speeds up Self-Reliance Process: Experts”. Global Times, 4 januari 2024, hämtad 3 januari 2025, *https://www.globaltimes.cn/page/202401/1304817.shtml*

”Different Fortunes in China as PC Shipments Fall 6% while Tablets Grow 20% in Q2 2024”. Canalys, 27 september 2024, hämtad 2 november 2024, *https://www.canalys.com/newsroom/china-pc-market-q2-2024*.

”Fortune Global 500: Information Technology Services”. Fortune, 3 oktober 2024, hämtad 3 oktober 2024, *https://fortune.com/ranking/global500/search/?sector=Retailing&fg500_industry=Information+Technology+Services*.

”Fortune Global 500: Technology”. Fortune, 3 oktober 2024, hämtad 3 oktober 2024, *https://fortune.com/ranking/global500/search/?sector=Technology*.

”Fortune Global 500: Telecommunications”. Fortune, 3 oktober 2024, hämtad 3 oktober 2024, *https://fortune.com/ranking/global500/search/?sector=Telecommunications&fg500_industry=Information+Technology+Services*.

”World’s First 1.2TB Ultra-High-Speed Backbone Network Ppens in China”. Global Times, 13 november 2023, hämtad 3 oktober 2024, *https://www.globaltimes.cn/page/202311/1301765.shtml*.

Allen, Gregory C. ”China’s New Strategy for Waging the Microchip Tech War”. Washington D.C.: Center for Strategic & International Studies, 2023, hämtad 4 januari 2025, *https://www.csis.org/analysis/chinas-new-strategy-waging-microchip-tech-war*.

Allen, Gregory C. ”China Is Striking Back in the Tech War With the U.S”. TIME, 20 juli 2023, hämtad 3 november 2024, *https://time.com/6295902/china-tech-war-u-s/*.

Andersson, Patrik, Björn Cappelin, Björn Jerdén, Denis Korneev, Frida Lindberg, Hillevi Pårup och Tommy Shih. ”Kommunistpartiets 20:e nationella kongress: Xi Jinping stärker sitt grepp om Kina”. Brief nr. 4 (Stockholm: Nationellt kunskapsscentrum om Kina, 2022), hämtad 4 oktober 2024, *https://kinacentrum.se/wp-content/uploads/2022/11/kommunistpartiets-20e-nationella-kongress-xi-jinping-starker-sitt-grepp-om-kina.pdf*.

Asiatiska utvecklingsbanken. ”The 14th Five-Year Plan of the People’s Republic of China – Fostering High-Quality Development”. Juni 2021, hämtad 3 oktober 2024, *https://www.adb.org/sites/default/files/publication/705886/14th-five-year-plan-high-quality-development-prc.pdf*

Au, Anson. ”Digitalization in China: Who’s Left behind?”. Information, Communication & Society, vol. 27, nr. 6 (2023): 1247–1265.

Bernstein, Drew. ”Who Is Winning the AI Arms Race?”. Forbes, 28 augusti 2024, hämtad 3 november 2024, *https://www.forbes.com/sites/drewbernstein/2024/08/28/who-is-winning-the-ai-arms-race/*.

Brady, Anne-Marie och Wang Juntao. ”China’s Strengthened New Order and the Role of Propaganda”. Journal of Contemporary China, vol. 18, nr. 62 (2009): 767–88.

Brics ministermöte för vetenskap, teknik och innovation (STI). ”Durban Declaration”. 3 juli 2018, 9 november 2024, *https://www.dsti.gov.za/images/BRICS-STI-Durban-Declaration-NEW-VERSION.docxFINAL-AGREED-VERSION.pdf*.

Brics institute för framtida nätverk (BIFN). ”About BIFN”. Hämtad 15 november 2024, *https://www.bifn.org/about.html*.

Brown, Kerry. CEO, China: The Rise of Xi Jinping. London och New York: I. B. Tauris, 2016.

Burell, Mattias och Kristina Sandklef. AI-Utvecklingen i Kina – Påverkan på den svenska tjänstemannasektorn. Stockholm: Futurion, 2022, hämtad 15 mars 2025, *https://futurion.se/wp-content/uploads/2022/10/futurion-rapport-ai-i-kina-2022-lowres.pdf*.

Campanella, Edoardo och John Haigh. ”The Battle for the Internet”, Survival, vol. 66, nr. 1 (2024): 69–84.

Cary, Dakota. China’s National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain, Issue Brief. Washington D.C.: Center for Security and Emerging Technology (CSET), 2021.

Chandel, Sonali, Zang Jingji, Yu Yunnan, Sun Jingyao och Zhang Zhipeng. ”The Golden Shield Project of China: A Decade Later—An in-Depth Study of the Great Firewall”. 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) (2019): 111–19.

Center for Security and Emerging Technology (CSET). ”The Central Committee of the Communist Party of China and the State Council issued the National Standardization Development Outline”. Xinuha News Agency, 10 oktober 2021, hämtad 12 november 2024, *https://cset.georgetown.edu/wp-content/uploads/t0406_standardization_outline_EN.pdf*

Cheng, Dean. Cyber Dragon: Inside China’s Information Warfare and Cyber Operations. Santa Barbara: Praeger, 2017.

Cheng, Joseph Y. S. ”China’s Approach to BRICS”. Journal of Contemporary China, vol. 24, nr. 92 (2015): 357–75.

Cheng, Jing och Jinghan Zeng. ”’Digital Silk Road’ as a Slogan Instead of a Grand Strategy”. Journal of Contemporary China, vol. 33, nr. 149 (2024): 823–38.

Cheung, Tai Ming. ”The Rise of China as a Cybersecurity Industrial Power: Balancing National Security, Geopolitical, and Development Priorities”. Journal of Cyber Policy, vol. 3, nr. 3 (2018): 306–26.

Chow, Daniel C. K. ”How China Promotes Its State-Owned Enterprises at the Expense of Multinational Companies Doing Business in China and in other Countries”. Ohio State Public Law Working Paper, nr. 307: 1–29.

Cimpanu, Catalin. ”Two of China’s largest tech firms are uniting to create a new ’domestic OS’”. Zdnet/International, 11 december 2019, hämtad 3 januari 2025, *https://www.zdnet.com/article/two-of-chinas-largest-tech-firms-are-uniting-to-create-a-new-domestic-os/*.

Creemers, Rogier. ”The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy”. Journal of Contemporary China, vol. 33, nr. 146 (2024): 173–88.

Curtis, Jesse S. ”Springing the ‘Tacitus Trap’: Countering Chinese State-Sponsored Disinformation”. Small Wars & Insurgencies, vol. 32, nr. 2 (2021): 229–65.

Dai, Xiudian. ”ICTs in China’s Development Strategy”. I China and the Internet: Politics of the Digital Leap Forward. red. Christopher R. Hughes och Gudrun Wacker. London och New York: Routledge, 2003.

De Angelo, Dena. ”Global Reach – The New Scale of Chinese Cyberthreats”. Palo Alto Networks, 26 juni 2025, hämtad 2 september 2025, https://www.paloaltonetworks.com/blog/2025/06/new-scale-chinese-cyberthreats/.

Doshi, Rush, Emily De La Bruyère, Nathan Picarsic och John Ferguson. China as a ”Cyber Great Power”: Beijing’s Two Voices in Telecommunications. Washington: Brookings, 2021, hämtad 5 november 2024, *https://www.brookings.edu/wp-content/uploads/2021/04/FP_20210405_china_cyber_power.pdf*.

Englund, Johan och Oscar Almén. Den hundraåriga folkrepubliken: En bedömning av Kinas utveckling och relation till USA mot 2050, FOI-R--5631--SE. Stockholm: Totalförsvarets forskningsinstitut, 2024.

Feingold, Spencer. ”Where is China’s Economy Headed?” World Economic Forum, 27 juni 2024, hämtad 8 oktober 2024, *https://www.weforum.org/agenda/2024/06/china-economic-outlook-growth-trade/*.

FN:s konferens om handel och utveckling. ”Digital Economy Report 2024: Shaping an Environmentally Sustainable and Inclusive Digital Future”. Förenta nationerna, 11 juli 2024, hämtad 2 januari 2025, *https://www.un-ilibrary.org/content/books/9789213589779*.

Freedom House. ”Freedom on the Net 2024: The Struggle for Trust Online”. Washington, DC: Freedom House, 2024, hämtad 7 januari 2025, https://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf.

Fung, Courtney J. ”China’s Use of Rhetorical Adaptation in Development of a Global Cyber Order: A Case Study of the Norm of the Protection of the Public Core of the Internet”. Journal of Cyber Policy, vol. 7, nr. 3 (2022): 256–74.

Goldenziel, Jill. ”China’s Anti-Espionage Law Raises Foreign Business Risk”. Forbes, 3 juli 2023, hämtad 1 november 2024, *https://www.forbes.com/sites/jillgoldenziel/2023/07/03/chinas-anti-espionage-law-raises-foreign-business-risk/*.

Griffith, James. The Great Firewall of China: How to Build and Control an Alternative Version of the Internet. London och New York: Zed Books, 2021.

Grünberg, Nis. ”China’s 14th Five-Year Plan – Strengthening the Domestic Base to Become a Superpower”. MERICS, 9 april 2021, hämtad 3 oktober 2024, *https://merics.org/en/comment/chinas-14th-five-year-plan-strengthening-domestic-base-become-superpower*.

Han, Pengfei, Wei Jiang och Danqing Mei. ”Mapping U.S.–China Technology Decoupling: Policies, Innovation, and Firm Performance”. Management Science vol. 70, nr. 12 (2024): 8386–8413.

Hannas, William C. och Huey-Meei Chang. ”Chinese Technology Transfer”. I China’s Quest for Foreign Technology: Beyond Espionage, red. William C. Hannas och Didi Kirsten Tatlow. London och New York: Routledge, 2021.

Heilmann, Sebastian. Red Swan: How Unorthodox Policymaking Facilitated China’s Rise. New York: Columbia University Press, 2018.

Hoffmann, Stacie, Dominique Lazanski och Emily Taylor. ”Standardising the Splinternet: How China’s Technical Standards Could Fragment the Internet”. Journal of Cyber Policy, vol. 5, nr. 2 (2020): 239–64.

Hong, Jin, Song Hong, Liangbing Wang, Yi Xu och Dingtao Zhao. ”Government Grants, Private R&D Funding and Innovation Efficiency in Transition Economy”. Technology Analysis & Strategic Management 27, nr. 9 (2015): 1068–96

Hooijmaaijers, Bas. ”The BRICS Countries’ Bilateral Economic Relations, 2009 to 2019: Between Rhetoric and Reality”. Sage Open, vol. 11, nr. 4 (2021): 1–16.

Hooijmaaijers, Bas, ”China, the BRICS, and the Limitations of Reshaping Global Economic Governance”. The Pacific Review, vol. 34, nr 1 (2021): 29–55.

Hong, Yu. ”Pivot to Internet Plus: Molding China’s Digital Economy for Economic Restructuring?”. International Journal of Communication, vol. 11 (2017): 1486-1506.

Huang, Ying och Maximilian Mayer. ”Power in the Age of Datafication: Exploring China’s Global Data Power”. Journal of Chinese Political Science, vol. 28, nr. 1 (2023): 25–49.

International Data Corporation (IDC). ”Chinese Smartphone Market Accelerates to 8.9procent Growth in 2Q24, Led by Chinese OEMs”. 26 juli 2024, hämtad 5 januari 2025, *https://www.idc.com/getdoc.jsp?containerId=prAP52467524*.

International Institute for Management Development. ”World Digital Competitiveness Ranking 2023”, hämtad 7 september 2024, *https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/*.

ITU-R. IMT Vision – Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond. M.2083-0, M Series, Geneve, 2015, hämtad 23 augusti, 2025, https://www.itu.int/dms_pubrec/itu-r/rec/m/r-rec-m.2083-0-201509-i!!pdf-e.pdf.

Jiang, Renai, Haoyue Shi och Gary H. Jefferson. ”Measuring China’s International Technology Catchup”. Journal of Contemporary China, vol. 29, nr. 124 (2020): 519–34.

Jiang, Tianjiao. ”The Shift of China’s Strategic Thinking on Cyberwarfare Since the 1990s”. Journal of Chinese Political Science, vol. 28, nr. 1 (2023): 127–49.

Jinping, Xi. ”Full text of President Xi’s speech at the Opening of Belt and Road Forum”. Belt and Road Forum for International Cooperation, 14 maj 2017, hämtad 3 januari 2025, *http://2017.beltandroadforum.org/english/n100/2018/0306/c25-1038.html*.

Jinping, Xi. ”Embracing a Broader View and Cutting Through the Fog of Challenges to Advance High-Quality Development of Greater BRICS Cooperation”. Utrikesdepartementet, Folkrepubliken Kina, 24 oktober 2024, hämtad 10 november 2024, *https://www.mfa.gov.cn/eng/xw/zyxw/202410/t20241023_11514804.html*.

Jolly, Dominique. The New Threat: China’s Rapid Technological Transformation. Cham: Palgrave Macmillan, 2022.

Kemp, Simon. ”Digital 2024: China”. DataReportal, hämtad 5 januari 2025, *https://indd.adobe.com/view/f46b0abd-2754-42a7-9519-4566f99e2e7e?allowFullscreen=true&wmode=opaque*.

Kinas informationscenter för internetnätverk. ”The 53rd Statistical Report on China’s Internet Development”. Mars 2024, hämtad 3 oktober 2024, *https://www.cnnic.com.cn/IDR/ReportDownloads/202405/P020240509518443205347.pdf*.

Lee, Brice Tseen Fu och Juan Pablo Sims. ”Legitimacy Through Diversity: China’s Leadership in the BRICS + Expansion for Global Balance”. Fudan Journal of the Humanities and Social Sciences, online first (2024): 1–38.

Lee, Caitlin. ”Winning the Cold Tech War”. Rand, Santa Monica, 17 augusti 2023, hämtad 3 november 2024, *https://www.rand.org/pubs/commentary/2023/08/winning-the-tech-cold-war.html*.

Lei, Tu. ”China Prepares to Pilot Opening-Up of Internet Data Centers: Minister”. Global Times, 8 mars 2024, hämtad 7 januari 2025, *https://www.globaltimes.cn/page/202403/1308482.shtml*.

Li, Guanying. ”Internet Censorship in China: A Functioning Digital Panopticon”. I Communications in Contemporary China: Orchestrating Thinking, red. Nicole Talmacs och Altman Yuzhu Peng. Abingdon och New York, 2024.

Li, Luzhou och Kui Zhou. ”When Content Moderation Is Not about Content: How Chinese Social Media Platforms Moderate Content and Why It Matters”. New Media & Society, online first (2024): 1–17.

Lim, Lionel. ”Huawei’s Homegrown Operating System, Launched after the Company Was Put on a U.S. Blacklist, May Soon Overtake Apple’s iOS in China”. Fortune, 4 januari 2024, hämtad 4 januari 2025, *https://fortune.com/asia/2024/01/04/huawei-homegrown-os-harmonyos-second-most-used-in-china-apple-ios/*.

Marukawa, Tomoo. ”The Evolution of China’s Industrial Policy and ‘Made in China 2025’”. I Chinese Politics and Foreign Policy under Xi Jinping: The Future Political Trajectory, red. Arthur S. Ding and Jagannath P. Panda. London och New York: Routledge, 2021.

McGee, Patrick. Apple in China: The Capture of the World’s Greatest Company. London and New York: Simon and Schuster, 2025.

Mhalla, Majdouline, Jiang Yun och Alireza Nasiri. ”Video-Sharing Apps Business Models: TikTok Case Study”. International Journal of Innovation and Technology Management, vol. 17, nr. 07 (2020): 1–25.

Mingyang, Tao. ”China’s Homegrown Operating System Sees Rapid Development as US’ Tech Assault Backfires”. Global Times, 10 augusti 2023, hämtad 4 januari 2025, *https://www.globaltimes.cn/page/202308/1296031.shtml*.

Ministeriet för vetenskap och teknik. ”China Participates in the First Meeting of the Steering Committee of BRICS Technology Transfer Center Network”. Folkrepubliken Kina, 22 juni 2022, hämtad 3 november 2024, *https://en.most.gov.cn/pressroom/202206/t20220622_181227.htm#*.

Mo, Liam och Brenda Goh. ”TikTok Owner ByteDance, DeepSeek Lead Chinese Push in AI Reasoning”. Reuters, 22 januari 2025, hämtad 26 januari 2025, *https://www.reuters.com/technology/artificial-intelligence/tiktok-owner-bytedance-deepseek-lead-chinese-push-ai-reasoning-2025-01-22*.

Mueller, Milton L. ”China and Global Internet Governance: A Tiger by the Tail”. I Access Contested: Security, Identity and Resistance in Asian Cyberspace, red. Ronald Deibert, John Palfrey, Rafal Rohozinski och Jonathan Zittrain. Cambridge: MIT Press, 2011.

Mueller, Alex och Christopher S. Yoo. ”Crouching Tiger, Hidden Agenda?: The Emergence of China in the Global Internet Standard-Setting Arena”. Federal Communications Law Journal, vol. 76, nr. 23–33 (2024): artikel nr. 143: 1–71.

Negro, Gianluigi. The Internet in China: From Infrastructure to Nascent Civil Society. Cham: Palgrave Macmillan, 2017.

Negro, Gianluigi, ”The Rising Role of China in the Promotion of Multilateral Internet Governance, 1994–2014”. I History of the International Telecommunication Union (ITU): Transnational techno-diplomacy from the telegraph to the Internet, red. Gabriele Balbi och Andreas Fickers. Oldenbourg: De Gruyter, 2020.

Perrault, Ray och Jack Clark. ”Artificial Intelligence Index Report 2024”. Stanford: Stanford University Human-Centered Artifical Intelligence (HAI), 2024. Hämtad 3 november 2024, *https://aiindex.stanford.edu/wp-content/uploads/2024/05/HAI_AI-Index-Report-2024.pdf*.

Proven, Liam. ”China’s openKylin 1.0 arrives. Our verdict? Not a bad-looking, er, Ubuntu remix”. The Register, 7 july 2023, hämtad 3 december 2024, *https://www.theregister.com/2023/07/07/openkylin_is_ubuntu/*.

Qiao-Franco, Guangyu. ”An Emergent Community of Cyber Sovereignty: The Reproduction of Boundaries?”. Global Studies Quarterly, vol. 4, nr. 1 (2024): 1–11.

Repnikova, Maria och Kecheng Fang. ”Authoritarian Participatory Persuasion 2.0: Netizens as Thought Work Collaborators in China”. Journal of Contemporary China, vol. 27, nr. 113 (2018): 763–79.

Richter, Felix. ”Amazon Maintains Cloud Lead as Microsoft Edges Closer”. Statista, 2 maj 2024, hämtad 8 oktober 2024, *https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/*.

Rühlig, Tim. Technical Standardisation, China and the Future International Order. Bryssel: Heinrich Böll Stiftung, 2020, hämtad 12 november 2024, *https://eu.boell.org/sites/default/files/2020-03/HBS-Techn%20Stand-A4%20web-030320.pdf*.

Rühlig, Tim. The Sources of China’s Innovativeness Why China’s ”Unstoppable” Innovation Powerhouse Might Falter, DGAP Analysis. Berlin: German Council of Foreign Relations, 2023, hämtad 1 november, *https://dgap.org/system/files/article_pdfs/DGAP%20Analysis%20No-5_October-2023_16pp.pdf*.

Santacreu, Ana Maria och Heting Zhu. ”What Does China’s Rise in Patents Mean? A Look at Quality vs. Quantity”. Economic Synopses, nr. 14 (2018): 1-2.

Schott, Lennart och Kerstin J. Schaefer. ”Acceptance of Chinese Latecomers’ Technological Contributions in International ICT Standardization — The Role of Origin, Experience and Collaboration”. Research Policy, vol. 52, nr. 1 (2023): 104656, 1–16.

Segal, Adam. ”The Coming Tech Cold War With China Beijing Is Already Countering Washington’s Policy”. Foreign Affairs, 9 september 2020, hämtad 3 november 2024, *https://www.foreignaffairs.com/articles/north-america/2020-09-09/coming-tech-cold-war-china*.

Sheehan, Matt och Jacob Feldgoise. ”What Washington Gets Wrong About China and Technical Standards”. Carnegie Endowment for International Peace, 27 februari 2023, hämtad 12 november 2024, *https://carnegieendowment.org/research/2023/02/what-washington-gets-wrong-about-china-and-technical-standards?lang=en*.

Sheehan, Matt, Marjory S. Blumenthal, and Michael R. Nelson. ”Three Takeaways From China’s New Standards Strategy”. Carnegie Endowment for International Peace, 28 oktober 2021, hämtad 12 november 2024, *https://carnegieendowment.org/research/2021/10/three-takeaways-from-chinas-new-standards-strategy?lang=en*.

Shen, Hong. China’s Tech Giants: Baidu, Alibaba, Tencent. Bonn och Berlin: Konrad Adenauer Stiftung, 2018, hämtad 3 oktober 2024, *https://www.kas.de/en/web/politikdialog-asien/single-title/-/content/chinas-tech-giganten-baidu-alibaba-tencent*.

Shim, Yongwoon och Dong-Hee Shin. ”Neo-Techno Nationalism: The Case of China’s Handset Industry”. Telecommunications Policy, vol. 40, nr. 2–3 (2016): 197–209.

Sinaga, Lidya Christin. ”Xi Jinping, ‘China Dream’, and Chinese Military Diplomacy to ASEAN”. JAS (Journal of ASEAN Studies), vol. 8, nr. 2 (2021): 173–90.

Slotta, Daniel. ”Cumulative Size of Chinese Data Centers from 2019 to August 2023”. Statista, 5 juli 2024, hämtad 24 januari 2025, *https://www.statista.com/statistics/1477965/china-size-of-data-centers/*.

Statcounter Globalstats. ”Operating System Market Share Worldwide Sept 2023 – Sept 2024”, hämtad 8 oktober 2024, *https://gs.statcounter.com/os-market-share*.

Submarine Cable Networks. ”China”, hämtad 9 januari 2025, *https://www.submarinenetworks.com/en/stations/asia/china*.

Tai, Zixue. The Internet in China: Cyberspace and Civil Society. London och New York: Routledge, 2006.

Tran, Hung. ”China and India Are at Odds Over BRICS Expansion”. Atlantic Council, 8 augusti 2023, hämtad 8 januari 2025, *https://www.atlanticcouncil.org/blogs/new-atlanticist/china-and-india-are-at-odds-over-brics-expansion/*.

Utrikesdepartementet i Kina. ”Hu Jintao Presides over and Delivers an Important Speech at the Third BRICS Leaders Meeting in Sanya, Hainan Province”. Kinas folkrepublik, 14 april 2011, hämtad 2 november 2024, *https://www.fmprc.gov.cn/eng/xw/zyxw/202405/t20240530_11317056.html*.

Utrikesdepartementet, ”President Xi Jinping Meets with Indian Prime Minister Narendra Modi”, Folkrepubliken Kina, 24 oktober 2024, hämtad 9 januari 2025, *https://www.mfa.gov.cn/eng/xw/zyxw/202410/t20241023_11514914.html*.

Voo, Julia, Irfan Hemani och Daniel Cassidy. ”National Cyber Power Index 2022”. Cambridge: Belfer Center, 2022. Hämtad 3 november 2024, *www.belfercenter.org/project/cyber-project.*

Weber, Valentin. ”How China’s Control of Information is a Cyber Weakness”. Lawfare, 12 november 2020, hämtad 3 november 2024, *https://www.lawfaremedia.org/article/how-chinas-control-information-cyber-weakness*.

Woo, Ryan. ”China Wants to Mobilise Entire Nation in Counter-Espionage”. Reuters, 2 augusti 2023, hämtad 1 november 2024, *https://www.reuters.com/world/china/china-wants-mobilise-entire-nation-counter-espionage-2023-08-01/*.

Wu, Fei, Cewu Lu, Mingjie Zhu, Hao Chen, Jun Zhu, Kai Yu, Lei Li, Ming Li, Qianfeng Chen, Xi Li, Xudong Cao, Zhongyuan Wang, Zhengjun Zha, Yueting Zhuang och Yunhe Pan. ”Towards a New Generation of Artificial Intelligence in China”. Nature Machine Intelligence, vol. 2, nr. 6 (2020): 312–16.

Wu, Mingshi, Jackson Sippe, Danesh Sivakumar, Jack Burg, Peter Anderson, Xiaokang Wang, Kevin Bock, Amir Houmansadr, Dave Levin, och Eric Wustrow, ”How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic”, 32nd USENIX Security Symposium (2023): 2653–70.

Xinhua News Agency. ”Xi Proposes Closer, More Solid BRICS Partnership”. China Daily, 16 juli 2014, hämtad 3 januari 2025, *https://www.chinadaily.com.cn/world/2014xibricssummit/2014-07/16/content_17802884.htm*.

Yang, Zeyi. ”China Just Announced a New Social Credit Law. Here’s What It Means”. MIT Technology Review, 22 november 2022, hämtad 23 augusti 2025, *https://www.technologyreview.com/2022/11/22/1063605/china-announced-a-new-social-credit-law-what-does-it-mean/*.

Yu-Hsin Lin, Lauren och Curtis J. Milhaupt. ”China’s Corporate Social Credit System: The Dawn of Surveillance State Capitalism?” The China Quarterly, nr. 256 (2023): 835–53.

Zhang, Ruichen. ”Negotiating Censorship through ‘Socialist Recoding’ on the Chinese Internet: Nuances and Potentialities in a Contested Cyberspace”. Information, Communication & Society, vol. 27, nr. 1 (2024): 126–42.

Zhou, Weifeng och Mario Esteban. ”Beyond Balancing: China’s Approach towards the Belt and Road Initiative”. Journal of Contemporary China, vol. 27, nr. 112 (2018): 487–501.

# 7. Sydafrika – en passiv och ambivalent vågmästarstat

*Anna Ida Rock*

Sydafrikas förhållningssätt till Brics präglas av landets historia och inrikespolitiska kontext. Landets utrikes- och säkerhetspolitik kan i hög grad ses som en förlängning av African National Congress (ANC) agenda. ANC ombildades från befrielserörelsen till politiskt parti efter apartheids fall och dominerade sydafrikansk politik från det första demokratiska valet 1994 till presidentvalet i maj 2024.[1] Som en förlängning av kampen mot apartheid utgjorde mänskliga rättigheter, demokrati och suveränitet stommen i den normativa utrikespolitik president Nelson Mandela (1994–1999) och efterföljande Thabo Mbeki (1999–2008) förde. Under deras ledning strävade Sydafrika efter att positionera sig som en stat som står upp emot förtryck, sociala orättvisor och intolerans runt om i världen.[2] Alliansfrihet utgjorde en hörnsten i utrikespolitiken, liksom panafrikanism, reform av det internationella systemet, liksom att porträttera Sydafrika som en central del av det globala syd och att främja goda relationer till alla länder men speciellt syd-syd-samarbete.[3]

## 7.1 Sydafrikas relation med Brics

Sydafrika blev medlem i Brics 2011, som ett resultat av hårt kampanjarbete av president Jacob Zumas (2009–2018) regering. Under sin tid som president styrde Zuma Sydafrika närmare Ryssland och Kina samtidigt som han intog en mer kritisk ton gentemot västvärlden. Zuma fortsatte att retoriskt lyfta mänskliga rättigheter och en Afrikafokuserad agenda, men intog i praktiken en mer intressedriven utrikespolitik fokuserad på ”Sydafrika först” och ekonomisk diplomati.[4]

Inom Brics driver Sydafrika bland annat frågor om ekonomisk utveckling, rättvis handel, energi och infrastruktursatsningar. Sydafrika har även framhävt vikten av gemensamma insatser för att hantera transnationella säkerhetsproblem såsom cyberbrottslighet, organiserad brottslighet och terrorism.[5] Men Brics är inte bara en central plattform för att främja ekonomiska och säkerhetsmässiga intressen utan utgör också en möjlighet att uppvisa en (symbolisk) identitet som en internationell aktör av växande betydelse samt befästa bilden av Sydafrika som en afrikansk ledare och företrädare för det globala syd i bredare bemärkelse.[6] Sydafrika motiverade sin kandidatur till Brics bland annat genom att lyfta sitt regionala inflytande och beskriva sig som en ekonomisk ”inkörsport till” och en ”röst för” Afrika.[7] Temat på Brics-toppmötet i Johannesburg 2023 – ”Brics och Afrika: Partnerskap för ömsesidigt accelererad tillväxt, hållbar utveckling och inkluderande multilateralism” – illustrerar Sydafrikas ambition att vilja främja möjligheterna för hela Afrika. Sydafrika ser också Brics som en viktig plattform för att stärka multilateralism och skapa en multipolär världsordning där makt inom

1 Russell Buchan och Joe Devanny, *South Africa's Cyber Strategy Under Ramaphosa: Limited Progress, Low Priority* (Washington DC: Carnegie Endowment for International Peace, 2024).

2 Fritz Nganje och Odilile Ayodele, ”South African Foreign Policy”, i *Oxford Research Encyclopedia of International Studies*, (26 maj 2021), 10.

3 Sydafrikas föreställning om alliansfrihet går tillbaka till den alliansfria rörelsen (*Non-Aligned movement*) som uppkom under kalla kriget. Pan-afrikansm är ett samlingsbegrepp för afrikanska sammanhållnings- och avkolonialiseringsrörelser. Folashadé Soulé-Kohndou, ”South Africa in the BRICS-Africa Relationship Ambitions, Challenges, and Paradoxes”, *Afrique contemporaine*, vol. 2013/4, nr. 248 (2013), 1; Jakkie Cilliers, *Life beyond BRICS? South Africa's future foreign policy interests*, (Institute for Security Studies, 8 juni 2017).

4 Fritz och Ayodele, ”South African Foreign Policy”, 14.

5 Cyril Ramaphosa, ”Statement by President Cyril Ramaphosa during the BRICS Summit Open Plenary Session, on the occasion of the XVI BRICS Heads of State Summit, Kazan, Russia”, 23 oktober 2024.

6 Både interna och externa kritiker har dock ifrågasatt till vilken grad Sydafrika kan agera som en företrädare för Afrika. Soulé-Kohndou, ”South Africa in the BRICS-Africa Relationship”, 6.

7 Soulé-Kohndou, ”South Africa in the BRICS-Africa Relationship”; Carmody Padraig ”South Africa: The Odd BRIC Out”, *The Fletcher Forum of World Affairs*, 13 februari 2013.

det internationella systemet fördelas mer jämlikt mellan länder i det globala nord och syd.[8]

Sydafrika har starka relationer med flera Bricsländer, särskilt Ryssland och Kina. ANC har historiska band till Ryssland som sträcker sig tillbaka till frihetskampen och under sittande president Cyril Ramaphosa (2018– ) har relationerna till Moskva fördjupats ytterligare. Kina är Sydafrikas största handelspartner, men relationen kännetecknas av ett betydande handelsunderskott – något som Sydafrika har uppmärksammat i olika forum. Vid Brics-toppmötet i Johannesburg 2023 enades länderna om att minska handelsunderskottet och främja sydafrikansk export till Kina.[9] Efter att Rysslands anfallskrig mot Ukraina inleddes i februari 2022 har Ramaphosas regering framhållit att Sydafrika följer sin tradition av alliansfrihet.[10]

ANC tappade efter 30 år egen majoritet i parlamentsvalet i maj 2024, vilket ledde till att Sydafrika styrs av en koalitionsregering, bland annat bestående av ANC och landets största oppositionsparti Democratic Alliance (DA). DA ses generellt som betydligt mer västvänligt än ANC och partiet har intagit en öppet kritisk hållning till Rysslands agerande i Ukraina.[11] ANC lär behålla kontrollen över utrikespolitiken, men koalitionen med DA kan tvinga fram en mer balanserad strategi för att navigera mellan väst och Brics, Ryssland och Kina. Denna balansakt kompliceras av Sydafrikas sedan länge ansträngda relation till USA. Under Donald Trumps andra mandatperiod har relationerna försämrats ytterligare, bland annat efter ogrundade påståenden om folkmord på vita i Sydafrika och beskedet att Sydafrika inte kommer att bjudas in G20-mötet i Miami 2026.[12] Spänningarna kan öka incitamenten för Sydafrika att fördjupa sitt engagemang i Brics och andra icke-västliga samarbeten.

## 7.2 Internets utveckling i Sydafrika

Den första internetuppkopplingen i Sydafrika etablerades 1991 mellan datoravdelningen på Rhodes universitet i Östra Kapprovinsen och internetpionjären Randy Bushs hem i Portland i USA.[13] Året efter blev internet tillgängligt i Sydafrika även för kommersiell och privat användning. Digitaliseringen skalades upp under slutet av 2010-talet. 2023 hade nästan 80 procent av de sydafrikanska hushållen minst en medlem med tillgång till internet på något sätt. Det kan jämföras med strax över 40 procent av hushållen tio år tidigare.[14] Eftersom få sydafrikaner har råd att köpa dyrare och mer avancerade enheter har introduktionen av billigare smarttelefoner på den sydafrikanska marknaden inneburit att allt fler kan använda internet.[15] En majoritet av internetanvändarna i Sydafrika ansluter således genom en mobiltelefon (72,6 procent), medan betydligt färre har en fast anslutning i hemmet (14,5 procent) eller har åtkomst till internet på sin arbetsplats (14 procent).[16]

### It för utveckling och den digitala klyftan

Internet och annan it-infrastruktur är i teorin prioriterade områden i Sydafrika – det inhemska policyramverket är generellt sett välutvecklat, men det råder stora brister när det kommer till implementering och efterlevnad.[17] Sydafrikas strategier och policyer för it-området indikerar inte att Sydafrika ämnar utöva makt mot andra stater på cyberområdet. Istället utgör ”it för utveckling” den grundläggande principen och styrning och investeringar inom området kan framförallt ses som medel för ANC att nå sina övergripande utvecklingsmål att

8 Sydafrikanska regeringens nyhetsbyrå, ”SA to work with BRICS countries to advance African agenda”, 9 mars 2023.
9 Seth Thorne, ”South Africa’s biggest trading partners”, *BussinessTech,* 23 juli 2024.
10 Cyril Ramaphosa, ”Address by President Cyril Ramaphosa on outcomes of the XV BRICS Summit”, Union Buildings, Tshwane, 3 september 2023. Kritiker menar att landets agerande – såsom den marinövning som hölls i sydafrikanska vatten tillsammans med Ryssland och Kina i februari 2023 – kan tolkas som stöd för Ryssland. Greg Mills och Ray Hartley. ”Ramaphosa’s Geopolitical Charade — the Unbearable Consequences of Misaligning”. The Brenthurst Foundation, 1 november 2024.
11 John Steenhuisen, ”Putin is your ally, Mr President, not South Africa’s”, Democratic Alliance, 23 oktober 2024.
12 Basillioh Rukanga, ”South Africa hits back after Trump says US won’t invite it for G20 next year”, *BBC*, 27 november 2025.
13 Rhodes University, ”The Internet in South Africa turns 25”, 17 februari 2016.
14 Leah Ngari och Shira Aliza Petrack, ”Internet Infrastructure in Africa”, *Empower Africa*, u.å.
15 Samsungtelefoner står för den största marknadsandelen (över 50 procent 2024) i Sydafrika, följt av Apple och Huawei. Men det finns också en uppsjö av kinesiska företag som erbjuder billigare smartphones, som Hisense, Xiaomi, Oppo, Vivo, Techno Mobile, Realme och Itel Mobile. Luke Fraser, ”Most popular smartphone brands in South Africa – Apple vs Samsung vs Huawei and more”, *Businesstech*, 12 mars 2024.
16 Sydafrikas statistikdepartement, *Sydafrikas allmänna hushållsundersökning 2023*, maj 2024, 53.
17 Senka Hadzic, ”South Africa’s Digital Transformation: Understanding the Limits of Traditional Policies and the Potential of Alternative Approaches”, *Computer Law & Security Review*, vol. 55, 2024.

leverera ekonomisk tillväxt, bekämpa fattigdom och arbetslöshet samt nå ökad inkludering och jämlikhet.[18]

Mänskliga rättigheter, jämlikhet och rättvisa är centrala värden för Sydafrika även på internetområdet. Det sydafrikanska samhället är fortfarande djupt ojämlikt och en ”digital klyfta” delar landet, där vissa delar av befolkningen både har tillgång till och behärskar ny teknik, medan andra står utan dessa möjligheter.[19] Tillgång till kommunikation och information beskrivs som en grundläggande mänsklig rättighet och att minska den digitala klyftan är en högt prioriterad fråga för den sydafrikanska regeringen, vilket återspeglas i landets strategier och policyer.[20]

Då bredband lyfts som ett prioriterat område i den nationella utvecklingsplanen från 2012 så antog regeringen 2013 en nationell bredbandspolicy, SA Connect, vars huvudsakliga syfte är att minska den digitala klyftan och säkerställa bred tillgång till internet i Sydafrika.[21] Regeringen använder också olika typer av reglering inom cyberområdet som en hävstång för social och ekonomisk utveckling och jämlikhet. Exempelvis tillkännagav Sydafrikas oberoende kommunikationsmyndighet 2023, att företag som förvärvar frekvensspektrumlicenser måste bidra till SA Connect bland annat genom att ansluta offentliga inrättningar och tillhandahålla avgiftsfri tillgång till offentliga webbplatser.[22] Ett annat exempel är att det sedan 31 mars 2021 är reglerat enligt sydafrikansk lag att licensierade leverantörer av kommunikationsnät och tjänster måste ha 30 procent ägande av historiskt missgynnade grupper (svarta, kvinnor, unga och personer med funktionshinder) för att få verka i Sydafrika.[23]

## Öppenhet och frihet på internet

Sydafrika är en konstitutionell demokrati där den politiska makten är uppdelad mellan regering, parlament och domstolar. Den sydafrikanska grundlagen garanterar rätten till tryckfrihet och yttrandefrihet, off-line och online. Den garanterar också rätten till tillgång till information som innehas av staten. Öppenhet och frihet på internet är således viktiga principer i de strategier och policyer som reglerar styrning av internet och internetinfrastruktur i Sydafrika. Det återspeglas bland annat i den nationella vitbok för it-området som presenterades 2016 och vars alla målsättningar vilar på en underliggande filosofi om ”öppenhet” – ”öppen tillgång, öppet internet och öppen regering”.[24]

Sydafrika är det enda av Brics-länderna vars internet rankas som ”fritt” i Freedom House årliga analys av internetfrihet runt om i världen. Av totalt 72 länder som rankades i 2024 års upplaga placerade sig Sydafrika på 22:a plats globalt och första plats i Afrika med en samlad poäng på 74 av 100.[25] Sydafrika har ett levande civilsamhälle och en stark kultur av protester och mobilisering, vilket även gäller på internet.[26] Den sydafrikanska staten saknar direkt kontroll över landets internetstamnät och dess anslutningar till det globala internet. Det har inte heller förekommit några avsiktliga störningar i internettrafiken och det finns inga tecken på att staten eller andra aktörer blockerar eller filtrerar internet eller försöker begränsa användandet av digitala hjälpmedel för medborgerlig mobilisering av olika slag.[27]

Enligt Freedom House finns dock vissa oroande tendenser rörande internetfrihet i landet, såsom spridande av hatretorik, desinformation och ”deepfakes”, i synnerhet i samband med valen 2019 och 2024.[28] Statlig övervakning av onlineaktiviteter och insamling och lagring av användardata ger också grund för viss oro enligt

18 Buchan och Devanny, ”South Africa’s Cyber Strategy”, 4; Enrico Calandro,”South African Digital Sovereignty at the Crossroad of Securitization and Development”, i Jiang Min och Luca Belli, red. *Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance. Communication, Society and Politics*, (Cambridge University Press, 2025), 86.

19 Samuel T Faloye och Nurudeen Ajayi, ”Understanding the Impact of the Digital Divide on South African Students in Higher Educational Institutions”, *African Journal of Science*, Technology, Innovation and Development, vol. 14, nr. 7 (2021): 1734–44.

20 Charley Lewis, ”A step closer to achieving a connected South Africa where no one is left behind”, *Oberoende kommunikationsmyndigheten i Sydafrika*, 31 mars 2023.

21 Hadzic, ”South Africa’s Digital Transformation”.

22 Lewis, ”A step closer”.

23 3 kap. § 2 i Lag om elektronisk kommunikation 36, 2005 [Uppdaterad 8 maj 2024].; Vem som klassificeras som svart fastställs i Sydafrikas lagstiftning om Broad-Based Black Economic Empowerment.

24 Sydafrikas departement för telekommunikation och postservice, ”National Integrated ICT Policy White Paper”, 4.

25 Freedom House, *Freedom on the Net 2024,* 27 november 2024.

26 Freedom House, *South Africa: Freedom in the World Country Report*, u.å.

27 Freedom House*, South Africa: Freedom on the Net 2024 Country Report,* u.å.

28 CIPESA, *State of Internet Freedom in Africa - 2024 Africa’s Electoral Democracy and Technology: Pitfalls and Promises*, september 2024, 31.

Freedom House. Sydafrika har också pekats ut som ett av de länder som använder den israeliska övervakningsmjukvaran Pegasus.[29]

Sydafrika fäster stor vikt vid frågor som rör datasuveränitet. Den första juli 2021 trädde Protection of Personal Information Act i kraft. Lagstiftningen syftar bland annat till att skydda individers rätt till integritet och reglera hanteringen av personuppgifter. Lagen är i hög grad inspirerad av den europeiska dataskyddsförordningen.[30]

Den 31 maj 2024 publicerade den sydafrikanska regeringen en nationell moln- och datapolicy, vilken också betonar datasuveränitet och syftar till att trygga att data som genereras inom landet förblir under lokalt ägandeskap. Sydafrikas försök att kontrollera data begränsas dock av bristande resurser och kapacitet. I ett utkast från 2021 av moln- och datapolicyn föreslogs exempelvis ett centralt statligt ägt datacenter för statliga tjänsters data. Förslaget mötte kraftig kritik, bland annat för att den sydafrikanska statsapparaten ansågs sakna nödvändiga resurser och expertis.[31] I den slutgiltiga texten förespråkas fortfarande en ”moln förststrategi” – att statliga myndigheter och enheter ska prioritera molntjänster som det primära alternativet för nya it-upphandlingar.[32] Dock ges utrymme för dessa institutioner att välja privata molnleverantörer.[33]

## Cybersäkerhet

Trots att cybersäkerhet är ett prioriterat område enligt den sydafrikanska regeringen så nedprioriteras frågan i realiteten då de stora socio-ekonomiska utmaningarna som landet står inför kommer högre upp på agendan.[34] Institutionella och juridiska ramverk finns i huvudsak på plats, men det saknas tillräcklig finansiering och effektiv implementering.[35] Dessa brister drabbar bland annat Sydafrikas satsningar på cyberförmåga inom den militära sektorn. Det sydafrikanska parlamentet godkände 2015 etablerandet av ett militärt cyberkommando. Underfinansiering har hindrat cyberkommandot från att utveckla egna avancerade cyberförmågor eller skaffa nödvändiga förmågor från annat håll.[36] I augusti 2023 hävdade hackergruppen Snatch att den hade attackerat Sydafrikas Försvarsdepartement och Försvarsmakt. Gruppen påstod sig bland annat ha stulit militära kontrakt, persondata och interna anropssignaler.[37] Den sydafrikanska regeringen har tillbakavisat uppgifterna, men sydafrikanska analytiker menar att det finns tecken på att attacken har inträffat och händelsen har lyfts som ett exempel på cyberkommandots bristande förmåga.[38]

Sydafrika är i likhet med många andra stater både en protagonist och ett offer för cyberspionage. Som tidigare nämnts, finns det bland annat indikationer på att Sydafrika har använt det israeliska spionprogrammet Pegasus men också uppgifter om att Rwanda har övervakat President Ramaphosas telefon med hjälp av just Pegasus. Edward Snowdens avslöjande 2013 om att brittisk underrättelsetjänst spionerat på sydafrikanska diplomater under G20-toppmötet 2009 väckte stor uppmärksamhet i Sydafrika och satte fokus på frågan om digital övervakning, ett extra känsligt ämne i landet med tanke på dess erfarenhet av statlig övervakning under apartheid.[39]

Cyberbrottslighet utgör ett allvarligt problem och Sydafrika är ett av Afrikas mest utsatta länder när det gäller cyberattacker. Under 2022 var Sydafrika det åttonde mest drabbade landet i världen av så kallade ransomwareattacker, attacker som krypterar det angripna it-systemets data och kräver en lösensumma för att återställa dem. I februari 2023 rapporterade itsäkerhetsföretaget Kapersky att de hade registrerat över

29 Freedom House, *South Africa: Freedom on the Net 2024.*

30 Luca Belli, ”Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation”, *The African Journal of Information and Communication*, nr. 28 (2021), 1–14.

31 Heather Irvine och John Paul Ongeso, ”South Africa: The National Policy on Data and Cloud – Some highlights”, *Bowmans,* 18 juli 2024.

32 Sydafrikas departement för kommunikation och digital teknik, ”Electronic Communications Act: National Data and Cloud Policy”, *Government Gazette*, 31 maj 2024, 21

33 Sydafrikas departement för kommunikation och digital teknik, ”Electronic Communications Act: National Data and Cloud Policy”, 20; Ndlovu Nkosinathi, ”State scraps plan for own cloud data centres”, *Techcentral*, 3 juni 2024.

34 Buchan och Devanny, ”South Africa’s Cyber Strategy”, 1.

35 US International Trade Administration, ”South Africa – Country Commercial Guide”, 19 september 2024.

36 Buchan och Devanny, ”South Africa’s Cyber Strategy”, 5.

37 Halcyon, ”Snatch attacks South African Department of Defence”, 21 augusti 2023.

38 Daily Maverick, ”SNATCHed – SANDF data leaked in cyberattack appears to be authentic, say cybersecurity analysts”, 6 september 2023; Jan Vermeulen, ”Department of Defence walks back ‘fake news’ statement about data breach”, *My Broadband*, 28 august 2023; Buchan och Devanny, ”South Africa’s Cyber Strategy”, 8.

39 Buchan och Devanny, ”South Africa’s Cyber Strategy”, 6.

300 ransomwarebaserade utpressningsförsök i landet under en enda vecka.[40] Även kritisk infrastruktur och statliga institutioner är hårt drabbade. Betydande exempel är attacker mot City Power (som förser Johannesburg med elektricitet) i juli 2019, Justitiedepartementet i september 2021, internetleverantören RSAWEB i februari 2023, statligt ägda Utvecklingsbanken för Södra Afrika (DBSA) i juni 2023 och Sydafrikas nationella provsvarshantering i juni 2024.[41] Den ryska hackergruppen Akira tros ha legat bakom attacken mot DBSA, medan det saknas offentliga uppgifter om vilka som låg bakom de övriga attackerna.[42]

Som ett svar på den ökande cyberbrottsligheten instiftade Sydafrika en ny cyberbrottslag 2021. Den anpassar Sydafrikas lagstiftning till internationella standarder och ger rättsliga ramar för att utreda, åtala och förebygga cyberrelaterade brott.[43] Mycket tyder dock på att denna typ av brottslighet kommer att fortsätta att öka i Sydafrika. Förutom de problem som lyfts ovan så utgör bristen på kvalificerad it-personal en stor utmaning inom cybersäkerhetsområdet och både sydafrikanska företag och myndigheter har stora svårigheter att hålla sin kompetens uppdaterad för att möta snabbt föränderliga och växande hot. Dessutom saknas resurser både inom privat och offentlig sektor för att köpa mer avancerade eller multipla säkerhetssystem.

## 7.3 Internets samtida tillstånd i Sydafrika

Under apartheidtiden hade statliga Telekom monopol på telefoni och infrastruktur och den sydafrikanska staten kontrollerade och begränsade telekommunikationen – speciellt gentemot den svarta delen av befolkningen.[44] Sedan dess har marknaden öppnats upp och aktörer som Vodacom, majoritetsägt av brittiska Vodafone, och sydafrikanska MTN har blivit ledande.[45] Sydafrika har idag en välutvecklad internetinfrastruktur i urbana områden. Däremot är framstegen mindre när det gäller att bygga ut fibernät och uppgradera infrastrukturen för internet i områden längre ifrån de stora städerna.[46] Utvecklingen av den digitala infrastrukturen, och därmed det *fysiska lagret* (se kapitel 2), i landet har till stor del skett tack vare privata inhemska och internationella operatörer, men den sydafrikanska staten har också spelat en betydande roll.[47]

Sydafrika har ett relativt omfattande och snabbt växande fiberoptiskt nätverk. I mitten av 2025 nådde fibernätet cirka 5,4 miljoner av Sydafrikas 19,5 miljoner hushåll.[48] Två av fibernätverksoperatörerna, Openserve, som är ett dotterbolag till halvstatliga Telekom, och privatägda Vumatel står för en marknadsandel på över 50 procent av de hushåll som både nås av och är anslutna till fiber.[49] Det finns också tio internetknutpunkter (IXP) (se kapitel 2) i Sydafrika och 54 procent av den lokala internettrafiken kan förmedlas via IXP:er i landet.[50]

I 2023 års *Network Readiness Index* rankades Sydafrika näst högst av alla afrikanska länder (efter Kenya), på plats 74 av 134 länder.[51] Den mobila nedladdningshastigheten är snabbast på kontinenten (och på plats 55 globalt sett).[52] Den sydafrikanska regeringen betonar gärna Sydafrikas välutvecklade digitala infrastruktur och lyfter landets roll som ”en regional hubb för digital trafik i Afrika”. En av de aspekter som lyfts fram av regeringen är de tio undervattenskablar som kopplar upp Sydafrika mot andra delar av världen – 2Africa, ACE, Equiano, SEACOM, WACS, SAT-3, SAFE, EASSy, METISS och T3.[53] De flesta av dessa ägs av olika konsortium av privata aktörer från olika

40 Simnikiwe Mzekandaba, ”Cyber crime’s annual impact on SA estimated at R2.2bn”, *ITWeb*, 4 april 2023; Interpol, *Interpol African Cyberthreat Assessment Report 2024*, april 2024, 23; Zawya, ”What to expect from South Africa’s cybersecurity landscape in 2024”, 18 mars 2024.

41 Interpol, *Interpol African Cyberthreat*, 13; Jonathan Grieg, ”State-owned bank in South Africa confirms ‘Akira’ ransomware attack”, *The Record,* 13 juni 2023; Jonathan Grieg, ”South Africa’s national health lab hit with ransomware attack amid mpox outbreak”, *The Record*, 25 juni 2024..

42 Calandro, ”South African Digital Sovereignty”, 94.

43 Government Gazatte, ”Act No. 19 of 2020: Cybercrimes Act, 2020”, vol. 672, nr. 44651 (1 juni 2021).

44 Robert B. Horwitz, ”South African telecommunications: history and prospects”, i *Telecommunications in Africa,* red. Eli M. Noam (New York: Oxford University Press, 1999), 213.

45 World Bank Group, *South Africa Digital Economy Diagnostic*, (Washington, DC: World Bank, 2019).

46 US International Trade Administration, ”South Africa – Country Commercial Guide”.

47 World Bank Group, *South Africa Digital Economy Diagnostic*.

48 Daniel Puchert, ”Next fibre gold rush in South Africa”, *My Broadband,* 10 juli 2025.

49 My Broadband, ”South Africa’s top fibre network operators revealed”, 16 augusti 2022.

50 Internet Society Pulse, ”IXP Tracker”, November 2024.

51 Soumitra Dutta och Bruno Lanvin (red.), Network Readiness Index 2023, (Portulans Institute, 2023).

52 Speedtest, ”Speedtest Global Index”, november 2024.

53 Sydafrikas departement för kommunikation och digital teknik, ”South Africa’s Communications & Digital Technology Infrastructure Roadmap”, 28–31 oktober 2024, 3.

länder.[54] Exempelvis ägs 2Africa av Bayobab (tidigare MTN Global Connect), China Mobile, Meta Platforms, Orange, Saudi Telecom, Telecom Egypt, Vodafone och WIOCC.[55] Equiano ägs däremot helt av Google och T3 av Mauritius Telecom, som i sin tur till största delen ägs av Mauritius regering.[56]

Förseningar av frekvensspektrumauktioner förhindrade länge en bred lansering av femte generationens mobiltelefoni (5G).[57] Under covid 19-pandemin använde Vodacom och MTN temporära spektrum för att under 2020 lansera de första större 5G-nätverken och därmed börja erbjuda 5G mobil- och FWA-tjänster (*fixed wireless access*, en variant av trådlöst bredband) i Sydafrika.[58] Efter att den första frekvensspektrumauktionen på 14 år hållits i mars 2022 började 5G-nätet snabbt expandera och bli tillgängligt i stora delar utav landet. År 2023 täcktes 38 procent av befolkningen av 5G-nätet, en ökning med nästan 20 procentenheter på bara ett år.[59] Sydafrikanska Rain lanserade 2020 i samarbete med Huawei landets första fristående nätverk, medan de andra stora aktörerna hittills framförallt använder icke-fristående nätverk.[60] De flesta samtal och meddelanden i Sydafrika hanteras dock fortfarande via 4G-nätet.[61]

Internet är tillgängligt i Sydafrika även via satellit, vilket möjliggör tillgång till internet även i områden där andra uppkopplingsmöjligheter saknas. Sydafrika är dock det enda landet i södra Afrika där Space X Starlink inte har fått tillstånd att tillhandahålla sina tjänster.[62] Förhandlingar pågår med Space X, men stötestenen tycks vara den lag som kräver 30 procent ägandeskap av historiskt missgynnade grupper för att Starlink ska få verka i landet. Det tycks dock finnas en stark vilja från den sydafrikanska regeringen att tjänsten ska kunna lanseras i landet och regeringsföreträdare har uttryckt att den aktuella lagen ska ändras.[63] Trots förmåga att designa, utveckla och bygga satelliter har Sydafrika ännu inga egna kommunikations- eller signalspaningssatelliter.[64]

Sydafrika är en av de ledande it-ekonomierna i Afrika. Kapstaden, Johannesburg och Pretoria utgör viktiga digitala innovationshubbar med hög koncentration av startuper.[65] Antalet företag inom mjukvaruutveckling och telekommunikation växer, liksom antalet globala it-företag som etablerar sig i Sydafrika. Även datacentermarknaden är under stark tillväxt och det finns ett fyrtiotal datacenter i Sydafrika. De flesta av dem är koncentrerade till Johannesburg, Kapstaden och Durban. Marknaden kännetecknas av hög konkurrens och består av en bredd av både lokala och internationella aktörer. Under de senaste åren har Sydafrika bland annat attraherat stora investeringar i datacenterinfrastruktur från flera internationella storföretag som Microsoft, Amazon Web Services, Google, Huawei och Oracle.[66]

## Begränsningar och beroenden

Trots en växande it-sektor begränsas Sydafrikas digitala utveckling av brist på expertis och både myndigheter och företag har svårt att rekrytera kvalificerad personal.[67] Det råder bland annat brist på högspecialiserad kompetens inom områden som cybersäkerhet, artificiell intelligens, dataanalys, DevOps (kombinerad utveckling och drift), systemdesign, datalagring och mjukvaruutveckling, vilket tvingar företag att lägga ut vissa av dessa roller på entreprenad till andra länder.[68] I *Global Skills Report* 2024 rankas Sydafrika på plats 100 av de

54 *South Africa: Freedom on the Net 2024.*

55 Biz News, ”Undersea cable chaos: Why South Africa’s internet is in crisis”, 19 mars 2024.

56 *South Africa: Freedom on the Net 2024.*

57 Hadzic, ”South Africa’s Digital Transformation”, 3.

58 Kenechi Okeleke och James Joiner, *5G in Africa 2023 Market status, trends and outlook*, (GSMA Intelligence, oktober 2023), 18.

59 Oberoende kommunikationsmyndigheten i Sydafrika, *The State of the ICT Sector Report of South Africa,* mars 2024.

60 International Finance, ”Rain deploys its first standalone 5G network in South Africa”, 20 juli 2020.

61 Paula Gilbert, ”South Africa pushes 2G, 3G sunset to 2027”, Connecting Africa, 4 juni 2024.

62 Det är möjligt att använda Starlink i Sydafrika via roaming om användaren registrerar sig i närliggande länder. Hanno Labuschagne, ”Starlink roaming cutoff survivors”, My Broadband, 16 oktober 2024.

63 Matshepo Sehloho, ”South Africa could amend law blocking Starlink entry”, *Connecting Africa*, 8 oktober 2024; etableringen kompliceras ytterligare av Starlinks ägare Elon Musk själv är från Sydafrika och har en konfliktfylld relation med ANC, se exempelvis Central News, ”Elon Musk Accuses South African Government of Racism Over Starlink License Denial Amid Blocked Free Internet Offer for Rural Schools”, 7 december 2025.

64 Regeringen offentliggjorde dock 2022 planer att utveckla en egen kommunikationssatellit. International Institute for Strategic Studies, *Cyber Capabilities and national power volume 2*, (u.å.), 133.

65 Disrupt Africa, *The South African Startup Ecosystem Report*, (2022).

66 Michelle Donegan, ”Data center investment on the rise in Africa”, *Inform*, 23 maj 2024.

67 Africa Analysis, *2024 IITPSA ICT Skills Survey*, (Institute of Information Technology Professionals, South Africa, oktober 2024) , 6.

68 Sibahle Malinga, ”SA’s IT skills gap sees employers prioritise skills over degrees”, *IT Web*, 29 oktober 2024; Africa Analysis, *2024 IITPSA ICT,* 5.

107 nationer som rangordnas utifrån sin personalkompetens, framförallt inom teknik och datavetenskap.[69]

Sydafrika är i stor utsträckning även beroende av import av mjukvara och hårdvara. Den inhemska produktionen av hårdvara som datorer, servrar och smarta telefoner är begränsad och dessa produkter importeras bland annat från USA, Kina, Taiwan, Indien, Europa och Vietnam.[70] Vad gäller det *logiska lagret* (se kapitel 2) är globala bolag som Microsoft, Google, Apple och Oracle dominerande inom operativsystem.[71]

De flesta sydafrikaner använder internet framförallt för socialt nätverkande. Enligt *South Africa Yearbook 2022–2023* så har Sydafrika 44 miljoner internetanvändare varav 35 miljoner är användare av sociala medier.[72] Även inom det här området är den utländska dominansen påtaglig. Facebook har flest användare, följt av Tiktok vars popularitet växer snabbt. Instagram, X, LinkedIn, Telegram, Pinterest, sydafrikanska 2Go, Tinder och Grindr återfinns på plats tre till tio av de mest använda sociala medier-plattformarna.[73] De tio mest använda plattformarna i Sydafrika för direktmeddelanden var under 2023 Whatsapp, Messenger, iMessage, X, Snapchat, Telegram, MoyaApp, 2Go och Skype.[74] Av dessa är endast 2Go och MoyaApp utvecklade i Sydafrika.

Den omfattande energi- och elförsörjningskris som Sydafrika är drabbat av utgör också ett stort hinder för landets digitala infrastruktur och tekniska utveckling. Produktionsunderskottet är så stort att det har resulterat i återkommande planerade strömavbrott, så kallade ”load-sheddings”, där elen stängs av i olika områden för att minska belastningen på elnätet.[75] Dessa avbrott leder till störningar i kritisk digital infrastruktur, höga kostnader för reservlösningar och att den digitala utvecklingen bromsas. Exempelvis meddelade MTN under 2023 att företaget skulle pausa investeringar i ny 5G-infrastruktur, för att istället förse existerande torn med reservkraft.[76]

## 7.4 Brics och Sydafrikas ambitioner på internetområdet

Sydafrika beskrivs ofta som en viktig men passiv ”vågmästarstat” i relation till reglering och styrning av internet och annan it-infrastruktur.[77] Sydafrikas försiktiga agerande återspeglas även inom Brics-samarbetet där landet inte heller tycks följa någon enhetlig strategi.[78] Landets ambitioner begränsas dessutom av bristande kapacitet och expertis jämfört med andra Brics-länder som Kina och Ryssland. På ett mer övergripande plan ser dock Sydafrika Brics som en arena för att främja landets nationella it-intressen och bygga partnerskap för tillväxt och utveckling.[79] Inom Brics lyfter Sydafrika bland annat frågor som att minska den digitala klyftan – inom och mellan länder – utveckling av digital infrastruktur, tillgång till ny teknik och samarbete kring cybersäkerhetsfrågor.[80] Sydafrika betonar bland annat vikten av tekniköverföring och kapacitetsuppbyggnad, både mellan Brics-länderna och från Brics-länderna till resten av Afrika.[81] Brics utgör på så sätt en möjlighet för Sydafrika att stärka sin nationella kapacitet och få tillgång till avancerad teknik från länder som Kina och Ryssland. Samtidigt uttrycker landet också en vilja att vara en mer aktiv aktör i utvecklingen av transformativ

69 Coursera, *Global Skills Report 2024*.

70 Se exempelvis: Volza, ”Mobile Phone Imports in South Africa – Market Size & Demand based on Import Trade Data”, 26 augusti 2024; Volza, ”Computer Parts Imports in South Africa – Market Size & Demand based on Import Trade Data”, 17 juli 2024; OEC, ”Computers in South Africa 2022”.

71 Myles Illidge, ”Most popular desktop operating systems in South Africa, *My Broadband,* 26 december 2024.

72 Andrew Partridge, Sandra Makumbirofa, Mpho Moyo, Nawal Omar och Abdiaziz Ahmed, After Access 2022–2023: Digital South Africa Post the Pandemic, Policy Paper 1 in the series: 2022–2023 African After Access Survey: Digital Africa Post the Pandemic. (Research ICT Africa, Cape Town, 2024); Sydafrikanska regeringen, ”Communications and Digital Technologies” i *South Africa Yearbook 2022–2023* (Pretoria: Government Communications, 2023), 6.

73 Ornico, *The SA Social Media Landscape Report 2024,* 6.

74 Ornico, *The SA Social Media Landscape Report 2024,* 67.

75 Andrew Harding, ”South Africa load-shedding: The roots of Eskom’s power problem”, *BBC*, 24 maj 2023.

76 Okeleke och Joiner, *5G in Africa 2023*, 18.

77 International Institute for Strategic Studies, ”Cyber Capabilities”, 133.

78 Buchan och Devanny, ”South Africa’s Cyber Strategy”, 2, 12.

79 Sydafrikas regering, ”Minister Mondli Gungubele hosts the BRICS Ministers of Communications’ Meeting 2023, 31 Jul to 4 Aug”, 28 juli 2023.

80 Alexander Ignatov, ”BRICS Agenda for Digital Sovereignty”, *Modern Diplomacy*, 14 februari 2024; Sydafrikas regering, ”Minister Mondli Gungubele”.

81 Sydafrikas regering, ”Minister Mondli Gungubele”.

teknik inom Brics och ”inte bara vara en konsument av teknik som utvecklats någon annanstans”.[82]

Som nämnts ovan kantas Sydafrikas cyberdiplomati utanför Brics av tvetydighet, något som bland annat demonstreras av landets ställningstagande inom FN-systemet.[83] År 2016 röstade Sydafrika tillsammans med bland annat Kina, Ryssland och Venezuela emot en resolution i FN:s råd för mänskliga rättigheter om ”främjande, skydd och åtnjutande av mänskliga rättigheter på internet”. Sydafrikanska företrädare försvarade beslutet bland annat med att sydafrikaner redan garanterats åsikts- och yttrandefrihet i landets konstitution och att ”[u]tövandet av rätten till åsikts- och yttrandefrihet inte är absolut” med hänvisning till de stora problem Sydafrika haft med rasistisk hatretorik på internet.[84] Två år senare röstade Sydafrika dock för en snarlik resolution.[85]

Sydafrika har varit en aktiv medlem både i FN:s Group of Governmental Experts och FN:s Open-ended Working Group, vilket är ett konkurrerande format initierat av Ryssland.[86] Landet tycks dock inte driva någon tydlig egen agenda i dessa forum.[87] Sydafrika har även deltagit i diskussionerna om ett nytt fördrag om cyberkriminalitet, ett fördrag som förespråkas av Ryssland, men verkar ha intagit en medlande roll mellan de två lägren för att försöka finna en gemensam lösning.[88] Sydafrika har dessutom skrivit på Budapestkonventionen om cyberbrottslighet, vilket generellt sett ses som ett västerländskt initiativ samt Afrikanska unionens (AU) konvention om cybersäkerhet och skydd av personuppgifter. Dock har ingen av konventionerna ratificerats i Sydafrika.[89]

Sydafrika har ännu inte presenterat någon nationell ståndpunkt om hur internationell lag bör tillämpas i cyberrymden. Det är dessutom otydligt om Sydafrika kommer att stödja den rådande flerpartsstyrningsmodellen (*multistakeholder-modellen)* till reglering och styrning av internet och annan it-infrastruktur eller gå på Kina och Rysslands linje som förordar mer statlig kontroll. Dock antog AU den 18 februari 2024 en gemensam afrikansk ståndpunkt om tillämpning av internationell lag i användning av informations- och kommunikationsteknik i cyberrymden.[90] Det är den första gemensamma regionala ståndpunkten av sitt slag i världen och Sydafrika är en av 55 afrikanska stater som står bakom den. I den betonas vikten av att cyberrymden ska hållas ”öppen, säker, stabil, tillgänglig och fredlig”. Den slår dessutom fast att internationell lag gäller i cyberrymden och innehåller skrivelser om mänskliga rättigheter och yttrandefrihet. AU definierar också suveränitet i cyberrymden och menar exempelvis att cyberspionage kränker målstatens suveränitet när den syftar till att nå data lagrade på servrar som finns inom dess territorium, oavsett om den därigenom orsakar några negativa konsekvenser eller inte.[91]

Sydafrika har även bilaterala överenskommelser inom cyberområdet. Vid sidan av Brics-toppmötet 2017 i Xiamen skrev Sydafrika på ett avtal med Ryssland om att upprätthålla internationell informationssäkerhet. De två länderna förband sig bland annat att samarbeta kring cyberhot och i cyberbrottsutredningar. Dessutom syftar avtalet till att närmare samordna ländernas förhållningsätt till frågor om internationell informationssäkerhet i internationella forum, såsom FN och Brics.[92]

Sydafrika har också anordnat dialoger om internet och annan it-infrastruktur tillsammans med Storbritannien i september 2021 och med Nederländerna i april 2022. I det gemensamma uttalandet efter dialogen med Nederländerna noterade båda länderna vikten av internationella mekanismer som bidrar till att hålla cyberrymden öppen, fri, stabil och säker.[93]

## 7.5 Slutsatser

Sydafrikas utrikes- och säkerhetspolitik präglas av en balansakt mellan ideal och intressen. Denna komplexitet speglas i Sydafrikas relationer till Brics och dess

82 Sydafrikas department för kommunikation och digital teknik, ”Media statement: Minister of Communications and Digital Technologies Hosts the Brics Ministers of Communications’ Meeting 2023”, 28 juli 2023.

83 International Institute for Strategic Studies, ”Cyber Capabilities”, 133.

84 Gareth van Zyl, ”Why SA voted against internet freedoms at the UN”, *News 24*, 5 juli 2016.

85 Freedom House*, South Africa: Freedom on the Net 2019 Country Report*, u.å.

86 Ignatov, ”BRICS Agenda for Digital Sovereignty”.

87 Buchan och Devanny, ”South Africa’s Cyber Strategy”, 12.

88 Buchan och Devanny, ”South Africa’s Cyber Strategy”, 13.

89 International Institute for Strategic Studies, ”Cyber Capabilities”, 133.

90 Afrikanska Unionen, *Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace, CAP*, 29 januari 2024.

91 Afrikanska Unionen, *Common African Position*, 3.

92 Rysslands utrikesdepartement, ”Press release on signing a cooperation agreement between the Government of the Russian Federation and the Government of the Republic of South Africa on maintaining international information security”, 4 september 2017.

93 Nederländernas utrikesdepartement, ”Joint Statement South Africa and the Netherlands: Cyber Policy Dialogue”, 6 april 2022.

medlemsländer. Brics ger Sydafrika möjlighet att främja sina ekonomiska intressen, samtidigt som medlemskapet stärker Sydafrikas roll som en global aktör och representant för Afrika. Brics utgör också en arena för att främja syd-syd-samarbete och påverka globala maktstrukturer för att nå en mer jämlik maktfördelning mellan det globala nord och syd. Det är tydligt att Sydafrika inte planerar att överge sina band till Ryssland, Kina och Brics. Sydafrika har samtidigt inget intresse av att bryta banden till västliga länder eller äventyra sina viktiga ekonomiska och kulturella relationer med dem. Därtill bidrar den infekterade relationen med USA och den inrikespolitiska situationen, där ANC nu samregerar med det betydligt mer västtillvända DA, till osäkerhet kring Sydafrikas framtida utrikes- och säkerhetspolitiska inriktning.

För Sydafrika utgör cyberområdet framförallt ett medel för att nå socioekonomisk utveckling och jämlikhet. Trots hög digitaliseringsgrad finns betydande skillnader i digital tillgång och kunskap mellan olika samhällsgrupper i Sydafrika. Brist på resurser, kapacitet och politisk vilja hindrar implementeringen av i grunden välutvecklade policyer och regelverk, bland annat inriktat på att minska den digitala klyftan. Landets beroende av importerad mjuk- och hårdvara underminerar dess digitala suveränitet, medan brist på expertis och en otillräcklig elförsörjning ytterligare försvårar den digitala utvecklingen.

Inom cyberområdet ser Sydafrika Brics en möjlighet att stärka sin digitala kapacitet och infrastruktur. Landet driver frågor om digital innovation, inkludering, tillgång till ny teknik för alla medlemsstater och åtgärder för att minska den digitala klyftan. Cyberattacker utgör ett stort och växande hot för Sydafrika, vilket gör cybersäkerhet till ett annat prioriterat område inom Brics. Sydafrikas cyberdiplomati, både inom och utanför Brics, är präglat av försiktighet och tvetydighet. Beroende på fråga och sammanhang understryker Sydafrika ibland vikten av samarbete och dialog med många olika intressenter för att skapa inkluderande lösningar. I andra fall tycks Sydafrika förespråka ett förhållningssätt där regeringar spelar en mer central roll i styrningen av internet och internetinfrastruktur. Sydafrikas hållning även i andra internationella internetfrågor framstår ofta som otydlig, vilket delvis tycks spegla landets avsaknad av en övergripande strategi för området.

Brics utvidgning väcker frågor om hur Sydafrikas roll inom gruppen kommer att utvecklas. Trots begränsad ekonomisk, militär och diplomatisk makt har Sydafrika haft relativt betydande inflytande som en symbolisk representant för Afrika och det globala syd. Hur denna roll påverkas av två ytterligare afrikanska medlemsstater återstår att se.

# Referenser

Africa Analysis. *2024 IITPSA ICT Skills Survey*. Institute of Information Technology Professionals, South Africa, oktober 2024. *https://www.iitpsa.org.za/wp-content/uploads/2024/10/2024-IITPSA-ICT-Skills-Survey-and-Research-Report.pdf*.

Afrikanska Unionen. *Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace. CAP*, 29 januari 2024, hämtad 10 oktober 2025. *https://papsrepository.africanunion.org/server/api/core/bitstreams/65bdfced-80d9-445b-b57f-31037616ccda/content*.

Belli, Luca. ”Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation”. *The African Journal of Information and Communication*, nr. 28 (2021), 1–14.

Buchan, Russell och Joe Devanny. *South Africa's Cyber Strategy Under Ramaphosa: Limited Progress, Low Priority*. Washington DC: Carnegie Endowment for International Peace, 2024.

Carmody, Padraig. ”South Africa: The Odd BRIC Out”. *The Fletcher Forum of World Affairs*, 13 februari 2013, hämtad 10 oktober 2025. *https://www.fletcherforum.org/home/2016/8/12/south-africa-the-odd-bric-out*.

Central News. ”Elon Musk Accuses South African Government of Racism Over Starlink License Denial Amid Blocked Free Internet Offer for Rural Schools”. 7 december 2025, hämtad 11 december 2025. *https://centralnews.co.za/elon-musk-accuses-south-african-government-of-racism-over-starlink-license-denial-amid-blocked-free-internet-offer-for-rural-schools*.

Cilliers, Jakkie. *Life beyond BRICS? South Africa's future foreign policy interests*. Institute for Security Studies, 8 juni 2017, hämtad 10 oktober 2025. *https://issafrica.s3.amazonaws.com/site/uploads/sar9.pdf.*

CIPESA. *State of Internet Freedom in Africa – 2024 Africa's Electoral Democracy and Technology: Pitfalls and Promises*. September 2024, hämtad 10 oktober 2025. *https://cipesa.org/wp-content/files/reports/State_of_Internet_Freedom_in_Africa_2024.pdf*.

Coursera. *Global Skills Report 2024*. hämtad 7 oktober 2024. *https://www.coursera.org/skills-reports/global/get-report.*

Daily Maverick.”SNATCHed – SANDF data leaked in cyberattack appears to be authentic, say cybersecurity analysts”. 6 september 2023, hämtad 10 oktober 2015. *https://www.dailymaverick.co.za/article/2023-09-06-snatched-sandf-data-leaked-in-cyberattack-appears-to-be-authentic-say-cybersecurity-analysts/*.

Disrupt Africa. *The South African Startup Ecosystem Report 2022*. Hämtad 10 oktober 2025. *https://www.22onsloane.co/wp-content/uploads/2022/07/The-South-African-Startup-Ecosystem-Report-2022.pdf*.

Donegan, Michelle. ”Data center investment on the rise in Africa”. *Inform*, 23 maj 2024, hämtad 10 oktober 2025. *Data center investment on the rise in Africa*.

Dutta, Soumitra och Bruno Lanvin (red.). *Network Readiness Index 2023*. (Portulans Institute, 2023). *https://download.networkreadinessindex.org/reports/nri_2023.pdf*.

Calandro, Enrico. ”South African Digital Sovereignty at the Crossroad of Securitization and Development”. I *Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance. Communication, Society and Politics,* red. Jiang Min och Luca Belli (Cambridge University Press, 2025): 81–102.

Faloye, Samuel T. och Nurudeen Ajayi. ”Understanding the Impact of the Digital Divide on South African Students in Higher Educational Institutions”. *African Journal of Science, Technology, Innovation and Development*, vol. 14, nr. 7 (2021): 1734–44.

Fraser, Luke. ”Most popular smartphone brands in South Africa – Apple vs Samsung vs Huawei and more”. *Businesstech*, 12 mars 2024, hämtad 10 oktober 2025. *https://businesstech.co.za/news/technology/759335/most-popular-smartphone-brands-in-south-africa-apple-vs-samsung-vs-huawei-and-more/*.

Freedom House. *Freedom on the Net 2024.* 27 november 2024, hämtad 10 maj 2025. *https://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf*.

Freedom House. *South Africa: Freedom in the World Country Report*. u.å., hämtad 10 maj 2025. *https://freedomhouse.org/country/south-africa/freedom-world/2024*.

Freedom House. *South Africa: Freedom on the Net 2019 Country Report*. u.å., hämtad 10 maj 2025. *South Africa: Freedom on the Net 2019 Country Report | Freedom House*

Freedom House. *South Africa: Freedom on the Net 2024 Country Report.* u.å., hämtad 10 juni 2025. *https://freedomhouse.org/country/south-africa/freedom-net/2024*.

Gilbert, Paula. ”South Africa pushes 2G, 3G sunset to 2027”. Connecting Africa, 4 juni 2024, hämtad 19 maj 2025. *https://www.connectingafrica.com/regulation/south-africa-pushes-2g-3g-sunset-to-2027*.

Government Gazette. ”Act No. 19 of 2020: Cybercrimes Act, 2020”. vol. 672, nr. 44651 (1 juni 2021). *https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf*.

Government Gazette. ”Protection of Personal Information Act (POPI Act), Section 72 Transfers of personal information outside Republic”, vol. 581, nr. 37067, 26 november 2013. *https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf*.

Grieg, Jonathan. ”South Africa’s national health lab hit with ransomware attack amid mpox outbreak”. *The Record*, 25 juni 2024, hämtad 10 maj 2025. *https://therecord.media/south-africa-lab-ransomware-mpox-outbreak*.

Grieg, Jonathan. ”State-owned bank in South Africa confirms ‘Akira’ ransomware attack”. *The Record,* 13 juni 2023, hämtad 10 maj 2025. *https://therecord.media/development-bank-of-southern-africa-akira-ransomware-attack*.

Hadzic, Senka. ”South Africa’s Digital Transformation: Understanding the Limits of Traditional Policies and the Potential of Alternative Approaches”. *Computer Law & Security Review,* vol. 55 (2024).

Halcyon. ”Snatch attacks South African Department of Defence”. 21 augusti 2023, hämtad 10 maj 2025. *https://www.halcyon.ai/attacks/snatch-attacks-south-african-department-of-defence*.

Harding, Andrew. ”South Africa load-shedding: The roots of Eskom’s power problem”. *BBC*, 24 maj 2023, hämtad 10 maj 2025. *South Africa load-shedding: The roots of Eskom’s power problem*.

Horwitz, Robert B. ”South African telecommunications: history and prospects”. I *Telecommunications in Africa*, red. Eli M. Noam. New York: Oxford University Press, 1999.

Ignatov, Alexander. ”BRICS Agenda for Digital Sovereignty”. *Modern Diplomacy*, 14 februari 2024, hämtad 10 maj 2025. https://moderndiplomacy.eu/2024/02/14/brics-agenda-for-digital-sovereignty/.

Illidge, Myles. ”Most popular desktop operating systems in South Africa”. *My Broadband,* 26 december 2024, hämtad 10 maj 2025. *https://mybroadband.co.za/news/software/574409-most-popular-desktop-operating-systems-in-south-africa.html*.

International Finance. ”Rain deploys its first standalone 5G network in South Africa”. 20 juli 2020, hämtad 10 maj 2025. *https://internationalfinance.com/telecom/rain-deploys-first-standalone-5g-network-south-africa/*.

International Institute for Strategic Studies. *Cyber Capabilities and national power volume 2.* (u.å.), hämtad 20 maj 2025. *https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2.pdf*.

Internet Society Pulse. ”IXP Tracker”. November 2024. Hämtad 10 maj 2025. *https://pulse.internetsociety.org/en/ixp-tracker/?country_code=ZA*.

Interpol. *Interpol African Cyberthreat Assessment Report 2024*. April 2024. *https://afripol.africa-union.org/resources/interpol-african-cyberthreat-assessment-report-2024*.

Irvine, Heather och John Paul Ongeso. ”South Africa: The National Policy on Data and Cloud – Some highlights”. *Bowmans,* 18 juli 2024, hämtad 10 maj 2025. *https://bowmanslaw.com/insights/south-africa-the-national-policy-on-data-and-cloud-some-highlights/*.

Jiang, Min och Luca Belli, red. *Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance*. Cambridge University Press, 2025.

Labuschagne, Hanno. ”Starlink roaming cutoff survivors”. *My Broadband*, 16 oktober 2024, hämtad 19 maj 2025. *https://mybroadband.co.za/news/broadband/565276-starlink-roaming-cutoff-survivors.html.*

Lewis, Charley. ”A step closer to achieving a connected South Africa where no one is left behind”. *Oberoende kommunikationsmyndigheten i Sydafrika*, 31 mars 2023, hämtad 10 maj 2025. *https://www.icasa.org.za/news/2023/a-step-closer-to-achieving-a-connected-south-africa-where-no-one-is-left-behind*.

Loni Prinsloo. ”Government can do more to support SA developers: minister”. *Tech central*, 6 oktober 2021, hämtad 10 maj 2025. *https://techcentral.co.za/government-can-do-more-to-support-sa-developers-minister/203157/*.

Malinga, Sibahle. ”SA’s IT skills gap sees employers prioritise skills over degrees”. *IT Web*, 29 oktober 2024, hämtad 20 maj 2025. *https://www.itweb.co.za/article/sas-it-skills-gap-sees-employers-prioritise-skills-over-degrees/WnpNgM21zjj7VrGd*.

Mills, Greg och Ray Hartley. ”Ramaphosa’s Geopolitical Charade — the Unbearable Consequences of Misaligning”. *The Brenthurst Foundation*, 1 november 2024, hämtad 10 maj 2025. https://www.thebrenthurstfoundation.org/news/ramaphosas-geopolitical-charade-the-unbearable-consequences-of-misaligning/.

My Broadband. ”South Africa’s top fibre network operators revealed”. 16 augusti 2022, hämtad 10 maj 2025. *https://mybroadband.co.za/news/fibre/449488-south-africas-top-fibre-network-operators-revealed.html.*

Mzekandaba, Simnikiwe. ”Cyber crime’s annual impact on SA estimated at R2.2bn”. *ITWeb*, 4 april 2023, hämtad 10 maj 2025. https://www.itweb.co.za/article/cyber-crimes-annual-impact-on-sa-estimated-at-r22bn/JN1gPvOAxY3MjL6m

Ndlovu Nkosinathi. ”State scraps plan for own cloud data centres”. *Techcentral,* 3 juni 2024, hämtad 10 maj 2025. *https://techcentral.co.za/state-scraps-plan-own-cloud-data-centres/245712/*.

Nederländernas utrikesdepartement. ”Joint Statement South Africa and the Netherlands: Cyber Policy Dialogue”. 6 april 2022, hämtad 20 maj 2025. *https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/diplomatic-statements/2022/04/06/south-africa-netherlands-cyber-policy-dialogue-joint-statement*.

Nganje, Fritz och Odilile Ayodele. ”South African Foreign Policy”. I *Oxford Research Encyclopedia of International Studies*. 26 maj 2021. Hämtad 20 december 2024, https://oxfordre.com/internationalstudies/view/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-611.

Ngari, Leah och Shira Aliza Petrack. ”Internet Infrastructure in Africa”. *Empower Africa*, u.å., hämtad 10 maj 2025. https://empowerafrica.com/internet-infrastructure-in-africa/.

Oberoende kommunikationsmyndigheten i Sydafrika. *The State of the ICT Sector Report of South Africa.* Mars 2024, hämtad 10 maj 2025. *https://www.icasa.org.za/uploads/files/The-State-of-the-ICT-Sector-Report-31-March-2024.pdf*.

OEC. ”Computers in South Africa 2022”. U.å., hämtad 21 januari 2025. *https://oec.world/en/profile/bilateral-product/computers/reporter/zaf*.

Okeleke, Kenechi och James Joiner. *5G in Africa 2023 Market status, trends and outlook*.(GSMA Intelligence, oktober 2023).

Ornico. *The SA Social Media Landscape Report 2024. https://ornico.co/wp-content/uploads/2024/06/The-SA-Social-Media-Landscape-Report-2024.pdf*.

Pandor, Nadeli. ”BRICS collaboration helps find solutions for challenges facing Global South”. *Sydafrikas ambassad i Teheran*, 27 april 2023,hämtad 5 december 2024. http://southafricanembassy.ir/brics-collaboration-helps-find-solutions-for-challenges-facing-global-south.

Partridge, Andrew, Sandra Makumbirofa, Mpho Moyo, Nawal Omar och Abdiaziz Ahmed. *After Access 2022-2023: Digital South Africa Post the Pandemic*, . Policy Paper 1 i serien 2022-2023 African After Access Survey: Digital Africa Post the Pandemic. (Research ICT Africa, Cape Town, 2024.)

Ramaphosa, Cyril. ”Statement by President Cyril Ramaphosa during the BRICS Summit Open Plenary Session, on the occasion of the XVI BRICS Heads of State Summit, Kazan, Russia”. 23 oktober 2024, hämtad 10 maj 2025. *https://dirco.gov.za/statement-by-president-cyril-ramaphosa-during-the-brics-summit-open-plenary-session-on-the-occasion-of-the-xvi-brics-heads-of-state-summit-kazan-russia-23-october-2024/*

Puchert, Daniel. ”Next fibre gold rush in South Africa”. *My Broadband,* 10 juli 2025, hämtad 10 oktober 2025.. *https://mybroadband.co.za/news/broadband/600896-next-fibre-gold-rush-in-south-africa.html*

Ramaphosa, Cyril. ”Address by President Cyril Ramaphosa on outcomes of the XV BRICS Summit”. Union Buildings, Tshwane, 3 september 2023, hämtad 10 maj 2025. *https://www.presidency.gov.za/address-president-cyril-ramaphosa-outcomes-15th-brics-summit-union-buildings-tshwane.*

Ramaphosa, Cyril. ”Welcome Remarks by BRICS Chair, President Cyril Ramaphosa, at the BRICS–Africa Outreach and BRICS Plus Dialogue”. 24 augusti 2023, hämtad 10 maj 2025. *https://dirco.gov.za/welcome-remarks-by-brics-chair-president-cyril-ramaphosa-at-the-brics-africa-outreach-and-brics-plus-dialogue-24-august-2023/*.

Rhodes University. ”The Internet in South Africa turns 25”. 17 februari 2016, hämtad 10 maj 2025. *https://www.ru.ac.za/informationandtechnologyservices/latestnews/theinternetinsouthafricaturns25.html.*

Rukanga, Basillioh. ”South Africa hits back after Trump says US won’t invite it for G20 next year”. *BBC,* 27 november 2025, hämtad 10 december 2025. *https://www.bbc.com/news/articles/cq8dq47j5y8o*

Rysslands utrikesdepartement. ”Press release on signing a cooperation agreement between the Government of the Russian Federation and the Government of the Republic of South Africa on maintaining international information security”. 4 september 2017, hämtad 10 maj 2025. *https://mid.ru/en/foreign_policy/international_safety/1551693*.

Sehloho, Matshepo.”South Africa could amend law blocking Starlink entry”. *Connecting Africa*, 8 oktober 2024, hämtad 10 maj 2025. *https://www.connectingafrica.com/regulation/south-africa-could-amend-law-blocking-starlink-entry*.

Soulé-Kohndou, Folashadé. ”South Africa in the BRICS-Africa Relationship Ambitions, Challenges, and Paradoxes”. *Afrique contemporaine,* vol. 2013/4, nr 248 (2013): 31–43.

Speedtest. ”Speedtest Global Index”. November 2024, hämtad 10 maj 2025. *https://www.speedtest.net/global-index*.

Steenhuisen, John. ”Putin is your ally, Mr President, not South Africa’s”. *Democratic Alliance*, 23 oktober 2024, hämtad 10 maj 2025. *https://www.da.org.za/2024/10/putin-is-your-ally-mr-president-not-south-africas*

Sydafrikanska regeringen. ”Communications and Digital Technologies” i *South Africa Yearbook 2022–2023.* Government Communications, Pretoria, 2023.

Sydafrikanska regeringens nyhetsbyrå. ”SA to work with BRICS countries to advance African agenda”. 9 mars 2023, hämtad 19 maj 2025.. *https://www.sanews.gov.za/south-africa/sa-work-brics-countries-advance-african-agenda.*

Sydafrikas department för internationella relationer och samarbete. ”Media Briefing By The Minister Of International Relations And Cooperation, Dr Naledi Pandor, On South Africa’s State Of Readiness To Host The Xv Brics Summit”. 7 augusti 2023, hämtad 10 maj 2025. *https://www.dirco.gov.za/wp-content/uploads/2023/08/MEDIAB1.pdf*.

Sydafrikas departement för kommunikation och digital teknik. ”Electronic Communications Act: National Data and Cloud Policy”. *Government Gazette*, 31 maj 2024, hämtad 10 maj 2025. *https://www.gov.za/sites/default/files/gcis_document/202406/50741gen2533.pdf*.

Sydafrikas departement för kommunikation och digital teknik. ”Media statement: Minister Of Communications And Digital Technologies Hosts The Brics Ministers Of Communications’ Meeting 2023”. 28 juli 2023, hämtad 19 maj 2025. *https://www.dcdt.gov.za/images/Minister-Speeches/Media_Statement_-_Minister_of_Communications_and_Digital_Technologies_Hosts_the_BRICS_Ministers_of_Communications_Meeting_2023.pdf*.

Sydafrikas departement för kommunikation och digital teknik. ”South Africa’s Communications & Digital Technology Infrastructure Roadmap 28–31 oktober 2024”. Hämtad 10 maj 2025. *https://www.dcdt.gov.za/images/Minister-Speeches/South_Africas_Communications__Digital_Technology_Infrastructure_Roadmap_28-31_October_2024_.pdf*.

Sydafrikas departement för telekommunikation och postservice. ”National Integrated ICT Policy White Paper”. *Government Gazette*, nr. 40325, 3 oktober 2016, hämtad 10 maj 2025. *https://www.gov.za/sites/default/files/gcis_document/201610/40325gon1212.pdf*.

Sydafrikas nationella planeringskommission. *National Development Plan 2030: Our future make it work*. U.å., hämtad 10 maj 2025. *https://www.gov.za/sites/default/files/gcis_document/201409/ndp-2030-our-future-make-it-workr.pdf*.

Sydafrikas regering. ”Minister Mondli Gungubele hosts the BRICS Ministers of Communications’ Meeting 2023, 31 Jul to 4 Aug”. 28 juli 2023, hämtad 20 maj 2025. *https://www.gov.za/news/media-advisories/conferences-summits-seminars-and-workshops/minister-mondli-gungubele-hosts*.

Sydafrikas statistikdepartement. *Sydafrikas allmänna hushållsundersökning 2023*. Maj 2024, hämtad 10 maj 2025. *https://www.statssa.gov.za/publications/P0318/P03182023.pdf*.

Thorne, Seth. ”South Africa’s biggest trading partners”. *BussinessTech,* 23 juli 2024, hämtad 10 maj 2025.

US International Trade Administration. ”South Africa - Country Commercial Guide”. 19 september 2024, hämtad 5 december 2024.*https://www.trade.gov/country-commercial-guides/south-africa-digital-economy*.

Van Zyl, Gareth. ”Why SA voted against internet freedoms at the UN”. *News 24*, 5 juli 2016, hämtad 11 december 2025. *https://www.news24.com/business/why-sa-voted-against-internet-freedoms-at-the-un-20160705-*

Vermeulen, Jan. ”Department of Defence walks back ”fake news” statement about data breach”. *My Broadband*, 28 august 2023, hämtad 10 maj 2025. *https://mybroadband.co.za/news/security/505750-department-of-defence-walks-back-fake-news-statement-about-data-breach.html*.

Volza. ”Computer Parts Imports in South Africa – Market Size & Demand based on Import Trade Data”. 17 juli 2024, hämtad 10 maj 2025. *https://www.volza.com/p/computer-parts/import/import-in-south-africa/*.

Volza. ”Mobile Phone Imports in South Africa – Market Size & Demand based on Import Trade Data”. 26 augusti 2024, hämtad 10 maj 2025. *https://www.volza.com/p/mobile-phone/import/import-in-south-africa/*.

World Bank Group. *South Africa Digital Economy Diagnostic*. Washington, DC: World Bank, 2019. *documents1.worldbank.org/curated/en/464421589343923215/text/South-Africa-Digital-Economy-Diagnostic.txt.*

World Population Review. ”Crime Rate by Country 2024”. Hämtad 5 december 2024. *https://worldpopulationreview.com/country-rankings/crime-rate-by-country*.

Zawya. ”What to expect from South Africa’s cybersecurity landscape in 2024”. 18 mars 2024, hämtad 10 maj 2025. *https://www.zawya.com/en/world/africa/what-to-expect-from-south-africas-cybersecurity-landscape-in-2024-qgu53dyd*.

# 8. Slutsatser – Brics framtida digitala samarbete

*Per-Erik Nilsson och Carolina Vendil Pallin*

I DEN HÄR RAPPORTEN söks svar på huruvida de ursprungliga Brics-länderna driver en gemensam agenda för att skapa ett framtida och separat Brics-internet. Det korta svaret på den frågan är nej. För att nyansera svaret diskuteras i det här kapitlet drivkrafter: säkerhetspolitiska sådana inom Brics; Brics-ländernas inrikespolitiska överväganden; samt hur teknikutvecklingen påverkar Brics-ländernas position inom Brics. I en översiktlig tabell presenteras de fem Bricsländernas position inom cyberområdet. Detta följs upp med en framåtblickande diskussion som tar i beaktande vissa centrala aspekter relaterat till utvecklingar i och mellan EU och USA beträffande cyberdomänens och internets framtid som en säkerhetspolitisk fråga. Såväl den säkerhetspolitiska som tekniska utvecklingen går snabbt och det finns därmed ett antal områden som det finns anledning att följa. Kapitlet avslutas med förslag på ytterligare forskning om Brics och cyberdomänen.

## 8.1 Geopolitiska och säkerhetspolitiska drivkrafter

Cyberfrågor har kommit att bli en central aspekt i länders säkerhetspolitiska överväganden. Att kunna påverka, reglera och samarbeta på cyberområdet är en säkerhetspolitisk tillgång och nödvändighet för alltfler länder. Även rent geografiska förutsättningar kombinerade med socioekonomiska förhållanden inverkar på enskilda länders beslut om samarbete på cyberområdet. Säkerhetspolitiska drivkrafter handlar om att internet har blivit en sammanflätad fråga för nationell och internationell säkerhet, på både det civila och militära området.

Som framgår i rapporten har dessa drivkrafter inte resulterat i ett separat Brics-internet, men en rad samarbeten inom cyberområdet pågår inom Brics. Under skrivandet av den här rapporten har dessutom en rad utvecklingar skett på den globala arenan som innebär att ett mer samordnat internet inom Brics som motpol till det västliga inte kan avfärdas. Särskilt kan USA:s handels- och tullpolitik och användandet av den amerikanska dominansen i internets fysiska och logiska lager för politiska påtryckningar leda till en ökad vilja att söka sig till en strategisk autonomi gentemot väst inom Brics.

Samtliga Brics-länderna som har analyserats i denna studie har också visat sig vilja minska västs dominans i internationella institutioner, men i olika grad. Det är möjligt att skönja två block inom Brics, där Ryssland och Kina driver på medan Brasilien, Indien och Sydafrika är mer motvilliga. De senare vill inte skada sina relationer med väst, men har gett uttryck för klara fördelar med att fördjupa Brics-samarbetet generellt. Brasilien som Sydafrika ser Brics som en möjlighet att hävda en särskild roll i sina respektive regioner. För Indien, men även Brasilien och Sydafrika, förefaller Brics-medlemskapet ha varit ytterligare en kanal för att kräva en större roll i världspolitiken generellt – bland annat i FN:s säkerhetsråd. Brasilien och Sydafrika har dock varit mindre entusiastiska över att utvidga Brics eftersom det minskar deras relativa roll i organisationen. För ett fördjupat digitalt samarbete behöver länderna fortsätta att se Brics som en tillgång och vilja använda Brics snarare än andra organisationer som forum. Med fler medlemmar ökar också risken för ytterligare konfliktytor inom Brics (t.ex. om Pakistan tas upp som fullvärdig medlem).

Ryssland har varit en drivande röst i Brics. Kriget mot Ukraina och den isolering från västliga samarbeten som det resulterat i gör att Moskva fortsatt kommer att driva på för ett ökat samarbete inom Brics, inklusive på det digitala området. Kina har såväl ekonomiska som teknologiska muskler som de andra länderna i nuläget saknar. För Peking förefaller Brics vara ett av flera verktyg för att öka kinesiskt inflytande i omvärlden, särskilt i det globala syd. För Kina är Brics ett komplement till Shanghaisamarbetet och Sidenvägen. Peking kan därmed vilja intensifiera sina ansträngningar för att genom bland annat Brics genomdriva förändringar av den globala styrningen av internet på ett sätt som gynnar kinesiska intressen. Cyberrelaterade frågor som it-infrastruktur, it-standarder och artificiell intelligens (AI) kommer att vara centrala i denna strävan. Ryssland samarbetar sedan många år med Kina på det området, bland annat i FN.

För såväl Ryssland som Kina kan det finnas säkerhetspolitiska skäl för att utvidga antalet länder som ingår i Brics. De är starka spelare inom Brics och ju fler länder som ingår desto starkare argument har de för att driva på

en förändring av världsordningen till förmån för kinesiska och ryska intressen. Samtidigt kan en organisation med fler medlemsländer ställa till problem för både Ryssland och Kina vad gäller att styra organisationen i en för dem gynnsam strategisk riktning. En alltför stark styrning från dem kan till exempel komma att utmana den rådande Brics-retoriken om multilaterala demokratiska principer. Med fler medlemsländer kan också konfliktlinjerna inom Brics komma att öka. Den existerande gränskonflikten mellan Indien och Kina innebär ett betydande hinder, men visst samarbete på cyberområdet har ändå varit möjligt för Indien inom Brics.

## 8.2 Inrikespolitiska drivkrafter

Varje Brics-land har en egen inrikespolitisk realitet och dynamik att ta hänsyn till på cyberområdet. Länderna är olika stora, med olika geografiska förutsättningar samt har olika stor befolkning och förutsättningar för ekonomisk tillväxt. Även respektive lands statsskick och inrikespolitiska utveckling skiljer dem åt. Ryssland och Kina är auktoritära länder som har infört betydande begränsningar av friheten på internet inom sina länder. Friheten är än så länge större i Brasilien, Indien och Sydafrika. Det innebär att det är svårt att se hur Brics-länderna skulle kunna enas om reglerna på ett Brics-internet.

Brasilien är ett till ytan stort land där geografin innebär att vissa områden är glesbefolkade. Landet har också identifierat digitalisering som en viktig drivkraft för att bekämpa fattigdom och för att utveckla landets ekonomi. Förutom att Brasilien räknar sig om en demokrati torde landet vilja bevara goda relationer med väst för att uppnå bästa möjliga villkor för digital teknologisk utveckling och tekniköverföring. Samtidigt är både Kina och Ryssland viktiga handelspartner. Kuppförsöket i januari 2023 (se kapitel 3, avsnitt 3.3) har också satt spår och Brasilien kommer att vilja använda reglering på internetområdet för att förhindra en upprepning av sådana försök att omkullkasta landets politiska ordning.

Ryssland framstår som det mest entusiastiska landet för utvecklingen av Brics-internet och samarbete på cyberområdet generellt. Liksom Brasilien har Ryssland vissa utmaningar med en stor geografisk yta och dessutom en befolkning som minskar. Lägg till detta att flera områden i norra Ryssland och i ryska Fjärran Östern är glest befolkade. Samtidigt har ett alltmer repressivt politiskt system gjort att Ryssland prioriterat att kontrollera och övervaka befolkningen – även när det sker på bekostnad av funktionalitet på internet samt till priset av långsammare teknologisk och ekonomisk tillväxt.

Indien har till skillnad från Ryssland en stor och växande befolkning på en betydligt mindre yta. Regeringen prioriterar digital rättvisa och utveckling som viktiga faktorer för en växande ekonomi. Indiens relation till Kina belyser, som nämnts ovan, en del av den problematik som genomsyrar Brics-samarbetet. Kina är landets viktigaste handelspartner samtidigt som det pågår en latent gränskonflikt. För landets befolkning har tillgången till internetuppkoppling ökat rejält de senaste femton åren. I takt med att Indiens politiska system fått fler auktoritära inslag ser regeringen också behov av ökad politisk kontroll på internet, som frekventa nedsläckningar av internet och censur i digitala medier i vissa delstater.

Kina är stort till ytan men har framför allt också en stor befolkning. Teknologisk och teknisk utveckling

**Tabell 8.1** Schematisk beskrivning av Bricsländernas position inom cyberområdet.

| Land | Motstånd mot väst eller balansering på digitala området? | Fritt internet eller övervakning och kontroll? | Egen förmåga i logiska och fysiska lagret? | Medlemskap i Brics för att… |
|---|---|---|---|---|
| Brasilien | Balansering | Delvis fritt (vissa restriktioner) | Begränsad förmåga i båda. | Spela en ledande roll i Latinamerika och få mer inflytande för globala syd |
| Ryssland | Motstånd mot väst | Övervakning och kontroll | Förmåga i logiska; bristande i fysiska | Motverka effekter av sanktioner. Hitta allierade i konfrontationen med väst. |
| Indien | Balansering | Delvis fritt (vissa restriktioner, ökande kontroll) | Viss egen förmåga i logiska; bristande i fysiska | Få mer inflytandeglobala syd. |
| Kina | Motstånd mot väst – främst USA | Övervakning och kontroll | Förmåga i båda. | Öka sitt inflytande för att vinna över USA. |
| Sydafrika | Balansering | Fritt | Bristande förmåga i båda. | Spela en ledande roll i Afrika, bekämpa fattigdom och få mer inflytande i globala syd. |

på cyberområdet har sedan decennier varit ett strategiskt utvecklingsområde och är fortsatt prioriterat som en ekonomisk drivkraft för landets långsiktiga tillväxt och internationella oberoende. Idag är Kina det enda Brics-landet som på allvar kan utmana USA på cyberområdet. Vidare visar Kina att en stark kontroll av internet, både tekniskt och innehållsmässigt, är möjlig utan att skapa ett separat internet.

Sydafrika är det minsta av de ursprungliga Bricsländerna, både till yta och folkmängd. Ekonomisk utveckling och fattigdomsbekämpning är viktiga faktorer när landet drar upp riktlinjerna för sin politik på det digitala området. På ett ideologiskt plan står dessutom värderingar om digital rättvisa och mänskliga rättigheter i centrum. Sydafrika är det enda Brics-landet som rankas som att det har ett fritt internet av Freedom House.

## 8.3 Teknisk och teknologisk utveckling som drivkraft

För alla ursprungliga Brics-länder är vidare utbyggnad av fysisk infrastruktur på cyberområdet uttalade mål och omfattande infrastrukturinvesteringar står för dörren. I deklarationen från Brics-toppmötet 2025 betonas vikten av ”gemensamma åtgärder inom området digital infrastruktur för att säkerställa integriteten, stabiliteten i funktionen och säkerheten inom de nationella segmenten av Internet, samtidigt som internetfragmentering undviks”.[1] Återigen är formuleringarna allmänna och utformade så att alla länder kan skriva under utan att förbinda sig till ett vägval. Deklarationen nämner utbyggnad av höghastighetssjökablar, satellitbaserad kommunikation och nästa generationens kommunikation och understryker vikten av fortsatt teknologisk och teknisk utveckling. Särskilt nämns AI, kvantumdatorer, robotik och sakernas internet (*Internet of Things*). Till vilken grad Brics-länderna går från ord till handling återstår att se. Kritiska frågor som de enskilda länderna sannolikt ställer sig handlar om risker i att bygga in sig i beroendeställningar till framförallt Kina, liknande de som många av dem idag har gentemot USA. Det är dessutom en fråga som sträcker sig från nationell strategisk nivå till den enskilde konsumenten (via t.ex. den så kallade leverantörsinlåsningen).

Brasilien fortsätter att hålla dörren öppen för såväl väst som Brics. USA förefaller ha utövat viss påtryckning för att undvika att Brasilien använder kinesiska lösningar när landet investerar i nästa generations infrastruktur för mobilkommunikation. Även om kinesiska leverantörer som Huawei inte formellt är uteslutna tycks villkoren begränsa ett framtida beroende av Kina på just det här området. Brasilien har dock även agerat för att minska riskerna för att t.ex. Starlink etablerar en monopolställning i landet för satellituppkoppling.

Ryssland är ett av få länder i världen som har egna applikationer i det logiska lagret, till exempel sociala medier och sökmotorer som konkurrerar framgångsrikt med globala tjänster som Facebook och Google inom landet. Invasionen av Ukraina 2022 har dessutom tvingat landet att utveckla egna operativsystem och annan programvara eftersom Ryssland inte längre får uppdateringar av dessa system. Samtidigt ligger Ryssland efter både västländer och ledande asiatiska länder i teknologisk och teknisk utveckling för det fysiska lagret. Att landet numera är föremål för omfattande sanktioner gör det än mer osannolikt att rysk industri skulle inhämta eller ens knappa in på andra länders försprång vad gäller till exempel halvledare och servrar. Brics är därmed en viktig kanal för Ryssland för att försöka minska de negativa effekterna av de västliga sanktionerna. Det kommer att bli en utmaning för Ryssland att bygga ut infrastrukturen för mobilkommunikation samtidigt som stora resurser måste gå till ett krig och upprustning. Ryssland kommer sannolikt att tvingas förlita sig på kinesisk infrastruktur och riskerar därmed att bygga in sig i ett beroende gentemot Kina på medellång till längre sikt. Detta utesluter dock inte att Ryssland kan utveckla spetskompetens på vissa digitala områden, exempelvis vad gäller implementering av viss AI för militära syften.

I Indien finns en debatt om att undvika att bygga in sig i ensidiga beroenden. Ett exempel är Starlink. Liksom Brasilien tycks Indien också i praktiken utesluta Kina som huvudleverantör av infrastruktur för mobilkommunikation. Indien är också ett land som har en stor befolkning och en växande it-sektor, inte minst när det gäller it-tjänster för västerländska företag, som även är viktig som exportinkomst för landet. På många områden är framtiden lovande för Indien som it-nation och det är inte självklart att ett mer formaliserat samarbete inom Brics är mest gynnsamt för att fortsätta den trenden.

Som har diskuterats i rapporten ligger Kina långt fram både i teknologisk utveckling och i teknisk implementering. Landet har förmåga att utveckla alltifrån egna programlösningar för det logiska lagret till att tillverka hårdvara och dessutom exportera sina tekniklösningar globalt. Kina har haft en långsiktig strategi för att skapa autonomi på cyberområdet och kan därmed också exportera lösningar till övriga Brics-länder. Det handlar generellt om lösningar som kan erbjudas till en

1 ”The Rio de Janeiro Declaration.”

lägre kostnad än västliga leverantörers, men som kan komma med ett högt pris för enskilda länders cybersäkerhet och säkerhetspolitiska autonomi.

Sydafrika är en ledande it-ekonomi i Afrika, med en växande startup-miljö samt tillväxt inom mjukvaruutveckling och telekommunikation. Samtidigt hämmas den teknologiska utvecklingen av brist på kvalificerad arbetskraft, svag elförsörjning och ett långtgående beroende av importerad hård- och mjukvara. För Sydafrika utgör Brics ett verktyg för att få tillgång till ny digital teknik. Därtill vill landet se en politik för att minska de digitala klyftorna internationellt. Trots ett väl utarbetat politiskt ramverk på området finns dock en betydande risk för att Sydafrika kommer att fortsätta att ligga efter de övriga ursprungliga Bricsländerna på cyberområdet.

## 8.4 Framåtblick

De olika faktorerna som vi har gått igenom ovan kan således driva de ursprungliga medlemsländerna att samarbeta närmare men också skapa sprickor i Brics. Ett växande Brics kan också göra att formatet blir mer attraktivt för vissa länder men mindre givande för andra, som för Brasilien och Sydafrika. För flera av Brics-länderna kommer en springande fråga att vara om Brics *rör sig från* väst eller *närmar sig* väst (se Tabell 8.1).

Här ska understrykas att väst inte är en homogen enhet. Den amerikanska presidentadministrationens utrikespolitik under Donald Trump är en utmaning inte bara för Brics-länder, utan även för USA:s partner och allierade.[2] Beträffande cyberområdet har frågan lyfts inom EU om eventuella risker med ett stort beroende av amerikanska it-bolag på cyberområdet.[3] Vidare kan en politik för ökad kontroll av innehållet på internet i USA och EU,[4] åtgärder som tidigare kanske främst har associerats med Kina och Ryssland, leda till sprickor mellan EU och USA.[5] Samma politik kan för Brics-länder utvecklas till en anledning att välja kinesiska lösningar i en ”pest-eller-kolera-logik”. Till detta ska läggas att några av Brics-länderna har utsatts för cyberspionage och påtryckningar på cyberområdet från USA.

Med åren har Brics-samarbetet utvecklats i viss mån på cyberområdet. Det finns dock en gräns för hur långt samarbetet kan gå. Om Brics blir ett tydligare verktyg för de resursstarkare länderna, som Kina, att öka sitt inflytande inom Brics och globalt riskerar attraktionen att minska för länder som Brasilien, Indien och Sydafrika. De senare har hittills sett organisationen som ett verktyg för att öka sin relativa tyngd internationellt och på sina respektive kontinenter. De är inte primärt intresserade av att byta ett beroende mot ett annat. Snarare har de sannolikt mycket att vinna på att fortsatt balansera sin utrikespolitik och sitt digitala teknikberoende mellan väst och länder som Ryssland och Kina; för Indien är målsättningen t.o.m. att minska landets digitala beroende av Kina.

Tankarna om ett separat Brics-internet som fördes fram inför Rysslands ordförandeskap må ha varit mer signalpolitik eller önsketänkande än konkret policy, men att helt avskriva ett närmare digitalt samarbete inom Brics vore dock oklokt, även om det för närvarande är svårt att se hur t.ex. Indien skulle kunna samarbeta med Kina om cybersäkerhetsfrågor. De drivkrafter som låg bakom att Brics initialt bildades har bland annat resulterat i en alternativ utvecklingsbank. Det återstår att se om samma krafter kan driva på en ökad fragmentering på cyberområdet globalt. Medan en utvecklingsbank för Indien innebär bistånd med kinesiskt kapital skulle ett närmare cybersamarbete potentiellt öka beroendet av Kina med ökade risker för Indien i termer av nationell säkerhet.

Redan idag har Ryssland, Kina och Indien utvecklat egna operativsystem och användargränssnitt för mobiler och i Rysslands och Kinas fall även för persondatorer. Det kommer att vara av vikt att följa trenden för vilka operativsystem som anammas av användare i olika länder. Än så länge dominerar amerikanska lösningar, men att välja den kostbara lösningen att gå över till andra operativsystem är en bra indikator på hur nationell säkerhet kan gå före kostnadseffektivitet. Samarbete kring en sådan övergång kan minska kostnaden. Det finns dessutom en misstänksamhet och inte sällan förbittring över hur väst har dominerat globala institutioner och då även på det digitala området, vilket också kan öka viljan att ta kostnader för att minska beroende av väst. USA:s roll i framväxten av ett globalt internet har varit central och ett fåtal amerikanska multinationella företag dominerar i mångt och mycket på den

2 Richard Fontaine och Gibbs McKinley, ”Losing the Swing States”, *Foreign Affairs*, 27 oktober 2025.

3 Theodore Christakis, ”When Governments Pull the Plug”, *Lawfare*, 25 september 2025; Mathieu Pollet, ”Trump Can Pull the Plug on the Internet, and Europe Can’t Do Anything about It”, *Politico*, 23 juni 2025.

4 Daniëlle Flonk, Markus Jachtenfuchs och Anke Obendiek, ”Controlling Internet Content in the EU: Towards Digital Sovereignty”, Journal of European Public Policy, vol. 31, nr. 8 (2024): 2316–2342; Naomi Nix och Will Oremus, ”Trump Is Complicating the GOP’s Anti-Censorship Campaign”, *The Washington Post*, 9 oktober 2025.

5 Se: Kenneth Propp, ”Talking Past Each Other: Why the US-EU Dispute over ’Free Speech’ Is Set to Escalate”, *Atlantic Council*, 15 augusti 2025.

internationella marknaden. Hur väst och inte minst USA väljer att agera kan påverka politiken i samtliga Brics-länder framöver.

## 8.5 Vidare forskning

Denna rapports genomgång av de ursprungliga Brics-ländernas politik på cyberområdet demonstrerar att det finns anledning att följa utvecklingen inom organisationen. Hur de nya Brics-länderna förhåller sig till samarbete på cyberområdet kommer att ha betydelse för hur Brasilien, Ryssland, Indien, Kina och Sydafrika ställer sig till närmare digital integrering inom Brics framöver. Vissa av de nya Brics-länderna, som t.ex. Iran, är mer i linje med Ryssland och Kina vad gäller behovet av att etablera kontroll och övervakning av internet inom respektive länder av regimsäkerhetsskäl. Om Brics till exempel etablerar mer formella institutioner på cyberområdet efter Rio-deklarationen 2025, bör även det vara en utveckling av intresse att följa nära.

Brics är dessutom endast ett av flera möjliga verktyg som länder som Kina och Ryssland använder sig av för att driva sin politik på cyberområdet. Att undersöka närmare, till exempel, samarbetet inom Shanghai Cooperation Organization och de olika SCO-medlemsländernas politik på området skulle komplettera bilden av regionala digitala samarbetsformat. Även en studie av hur olika länder samarbetar med Kina inom ramen för den så kallade digitala sidenvägen är ett möjligt framtida forskningsämne.

Rapporten har identifierat att de val som de olika Brics-länderna gör när de investerar i digital infrastruktur kommer att bestämma vilka beroenden de försätter sig i. Samtidigt kommer säkerhetspolitiska avvägningar troligen också att styra infrastrukturval och i sin tur bestämma huruvida internets logiska och fysiska lager kommer att gå mot ökad fragmentering. Att följa denna fråga kommer att vara av stor vikt för att förstå vilket säkerhetspolitiskt handlingsutrymme länder har, men också potentiellt för att följa digital teknikutveckling utanför en västlig teknologisfär.

# Referenser

”The Rio de Janeiro Declaration”, Brics, 6 juli 2025, hämtad 5 oktober 2025, *http://brics.br/en/documents/presidency-documents/250705-brics-leaders-declaration-en.pdf*.

Christakis, Theodore. ”When Governments Pull the Plug”. *Lawfare*, 25 september 2025, hämtad 5 oktober 2025, *https://www.lawfaremedia.org/article/when-governments-pull-the-plug*.

Flonk, Daniëlle, Markus Jachtenfuchs och Anke Obendiek. ”Controlling Internet Content in the EU: Towards Digital Sovereignty”. *Journal of European Public Policy*, vol. 31, nr. 8 (2024): 2316–42

Fontaine, Richard och Gibbs McKinley. “Losing the Swing States”, *Foreign Affairs*, 27 oktober 2025, hämtad 7 november 2025, *https://www.foreignaffairs.com/united-states/losing-swing-states*.

Pollet, Mathieu. ”Trump Can Pull the Plug on the Internet, and Europe Can’t Do Anything about It”. *Politico*, 23 juni 2025, hämtad 5 oktober 2025, *https://www.politico.eu/article/donald-trump-eu-internet-europe-us-trade-war-data-cyber/*.

Nix, Naomi och Will Oremus. ”Trump Is Complicating the GOP’s Anti-Censorship Campaign”. *The Washington Post*, 9 oktober 2025, hämtad 9 oktober 2025, *https://www.washingtonpost.com/technology/2025/10/09/censorship-republicans-democrats-first-amendment/?_pml=1*.

Propp, Kenneth. ”Talking Past Each Other: Why the US-EU Dispute over ’Free Speech’ Is Set to Escalate”. *Atlantic Council*, 15 augusti 2025, hämtad 5 oktober 2025, *https://www.atlanticcouncil.org/blogs/new-atlanticist/us-eu-dispute-over-free-speech-is-set-to-escalate/*.

# Förkortningar

| Förkortning | Förklaring | Anm. |
|---|---|---|
| 4G | Fjärde generationens mobiltelefoni | En ny generation av Telekom skapas när teknikskiften är så stora att nya internationella standarder måste antas. |
| 5G | Femte generationens mobiltelefoni | |
| 5Gi | En av fyra teknologistandarder för 5Gi (indisk) | |
| ABIN | Brasiliens underrättelsemyndighet | Agência Brasileira da Inteligência |
| AI | Artificiell intelligens | |
| AIIB | Asiatiska infrastrukturinvesteringsbanken | Asian Infrastructure Investment Bank |
| ANC | Sydafrikanskt politiskt parti | African National Congress |
| Arpanet | Föregångaren till internet, utvecklad vid ARPA (USA:s försvarsforskningsmyndighet), från 1972 DARPA (Defence Advanced Research Projects Agency) | |
| Asean | En politisk samarbetsorganisation för länder i sydostasien | The Association of Southeast Asian Nations |
| AU | Afrikanska unionen | |
| BJP | Indiska folkpartiet | Bharatiya Janata Party |
| BNP | Bruttonationalprodukt | |
| Brics | Förkortning för länderna Brasilien, Ryssland, Indien, Kina och Sydafrika | |
| Brics+ | De ursprungliga Brics-länderna plus de som trätt in i Brics efter 2024; totalt nio medlemsländer från och med den 1 januari 2024. | Brasilien, Ryssland, Indien, Kina, Sydafrika, Egypten, Etiopien, Iran och Förenade Arabemiraten (Saudiarabiens anslutning är fortsatt oklar) |
| BSNL | Det statliga indiska telekombolaget | Bharat Sanchar Nigam Ltd. |
| CDCiber | Brasiliens nationella center för cyberförsvar | Centro de Defesa Cibernét |
| CERNET | Ett av de första sammankopplade nätverken i Kina. Se även CSTNet. | China Education and Research Network |
| CERT | Ursprungligen benämning på organisationer eller grupper som hanterar it-incidenter Numera ett varumärke som kräver tillstånd av Carnegie Mellon-universitetet | Computer Emergency Response Team |
| CIA | Amerikanska utrikesunderrättelsetjänsten | Central Intelligence Agency |
| ComDCiber | Brasiliens nationella cyberkommando | Comando de Defesa Cibernética |
| CSIRT | Benämning på organisationer och grupper som hanterar it-säkerhetsincidenter. Tillkom efter att CERT blivit ett varumärke. | Computer Security Incident Response Team |
| CSTNet | Ett av det första sammankopplade nätverken i Kina. Se även CSTNet. | China Science and Technology Network |
| CTF | Tävling för att hitta något som har dolts i ett it-system, t.ex. sårbarheter i program | Capture-the-flag |
| DA | Sydafrikanskt parti | Democratic Alliance |
| DBSA | Utvecklingsbanken för Södra Afrika | Development Bank of Southern Africa |
| DevOps | Kombinerad utveckling och drift av mjukvara | Development and operations |
| DNS | En internettjänst som översätter människoläsliga internetadresser, som example.com till datoradresser som 93.184. 216.34 (IPv4) och 2606:2800:220:1:248:1893:25c8:1946 (IPv6). | Domain Name System |
| DPDPA | Indisk lag om skydd av data | Digital Personal Data Protection Act |
| EU | Europeiska unionen | |
| Eximbank | Amerikanska export och importbanken | |
| Finep | Brasilianska innovationsfinansieringsmyndigheten | |
| FN | Förenta nationerna | |

| Förkortning | Förklaring | Anm. |
|---|---|---|
| FWA | En variant på trådlöst bredband | Fixed wireless access |
| G8 | Informell gruppering bestående av ledande industrinationer: Frankrike, Italien, Japan, Kanada, Ryssland, Storbritannien, Tyskland och USA (Ryssland uteslöts 2014 och formatet blev G7) | |
| G20 | Informell gruppering av de största ekonomierna globalt (samtliga Bricsländerna ingår) | |
| GDPR | EU:s dataskyddsförordning | General Data Protection Regulation |
| GGE | Arbetsgrupp med ansvar för att ta fram riktlinjer för global styrning av internet inom FN (endast ett begränsat antal länder deltar) | Group of Governmental Experts |
| GCHQ | Storbritanniens signalunderrättelsemyndighet | General Communications Headquarters |
| GSI | Det brasilianska kansliet för den nationella säkerhetsrådgivaren | Gabinete de Segurança Institucional |
| ETSI | Organisation som fastställer standarder för telekommunikation | European Telecommunications Standards Institute |
| HTML | Språk som används för att skriva webbsidor | Hypertext markup language |
| ICANN | Organisation som ansvarar för adressystemet på internet (se även DNS) | Internet Corporation for Assigned Names and Numbers |
| IANA | Organisation tilldelar nummer (t.ex. IP-adresser) på internet | Internet Assigned Numbers Authority |
| IEEE | Fastställer standarder inom elektronik och datateknik. | Institute for Electrical and Electronics Engineers |
| IETF | Internets tekniska ledningsgrupp | Internet Engineering Task Force |
| IKT | Informations- och kommunikationsteknik | |
| IMF | Internationella valutafonden | International Monetary Fund |
| IP | Internetprotokollet hanterar vissa funktioner i datatrafiken över internet. Däribland adressering av IP-paket. Ett av flera i internetprotokollsviten. | Internet protocol |
| IP-packet, packet, paket | IP-paket är en bit av ett meddelande som sänds över internet med internetprotokollet. I datakontext kallas de ofta bara paket. | Se IP |
| ISO | Internationella standardiseringsorganisationen | International Organization for Standardization |
| ISP | Internetleverantör | Internet service provider |
| IT | Informationsteknologi | |
| ITU | Internationella teleunionen (FN-organ) | International Telecommunication Union |
| IXP | Internetknutpunkt för att internetleverantörer ska kunna utbyta data direkt med varandra (peering) (se även POP) | Internet Exchange Points |
| MTN | Sydafrikanskt telekombolag | |
| Nfsnet | Multinationell mobiloperatör och internetleverantör med huvudkontor i Sydafrika | National Science Foundation Network |
| NSA | Nationella säkerhetsmyndigheten, USA:s signalspaningsunderrättelsemyndighet | National Security Agency |
| OECD | Organisationen för ekonomiskt samarbete och utveckling | Organisation for Economic Co-operation and Development |
| OEWG | Större arbetsgrupp för cyberfrågor i FN (ryskt initiativ och alla länder som vill delta är välkomna) | Open-ended Working Group |
| PND | Sammanfattande policydokument för Brasiliens nationella försvarspolitik | Política Nacional de Defesa |
| POP | Internetknutpunkt för en internetleverantörs kopplingar mot slutkunder och lokala telekomnät. (se även IXP) | point of presence |
| Protokoll | Uppsättning regler och format för hur datatrafik ska skickas och tas emot i ett datanätverk. (Se t ex IP) | |
| protokollsvit | En grupp av protokoll som används i samverkan för att hantera en kommunikationsstandard. Tex Wi-Fi. | |

| Förkortning | Förklaring | Anm. |
|---|---|---|
| Quad | Säkerhetspolitiskt samarbete mellan USA, Japan, Indien och Australien | Quadrilateral Security Dialogue |
| RAW | Indiens externa underrättelsemyndighet | Research and Analysis Wing |
| RIC | Samarbetsforum för politiska frågor mellan Ryssland, Indien och Kina | Russia–India–China |
| RosNIIROS | Forskningsinstitut som bildades som en del av Kurtjatovinstitutet; ansvarar för forskningsnätverk och grundläggande element av utvecklingen av det ryska segmentet av internet | Rossijskij nautjno-issledovatelskij institut razvitija obsjtjestvennych setej |
| 5G SA | Fristående 5G –nät som byggts endast för 5G, dvs. som inte använder existerande 4G-nät. | standalone |
| SCO | Shanghaisamarbetet är en mellanstatlig organisation för samarbete bland medlemsländer i Central- och Östasien | Shanghai Cooperation Organization |
| SDO | Formella organisationer som skapar standarder för produkter, tjänster eller processer | Standards development organizations |
| SSIC | GSI:s sekretariat för frågor om informations- och cybersäkerhet (Brasilien, se ovan under GSI) | Secretaria da Segurança da Informação e Cibernética |
| TCP/IP | Internets grundläggande protokollsvit | Transmission control protocol/ Internet protocol |
| UNGA | Förenta nationernas generalförsamling | General Assembly of the United Nation |
| USB | Standard för datatransmission och ström via en USB-kontakt | Universal serial bus |
| USB-kontakt | Kabel eller uttag för USB-användning. Inte märkesspecifik | |
| VK | Rysk social-media-applikation | Tidigare vKontakte |
| VPN | En krypterad internetanslutning som möjliggör nätverkstrafik vars innehåll och avsändare inte kan avlyssnas av obehöriga. | Virtual private network |
| VTC-program | | |
| W3C | Organisation som fastställer standarder för webbläsare, webbservrar och program för webben. | World Wide Web Consortium |
| Wi-fi | Namn för en protokollsvit för trådlös datakommunikation via radio | Inte förkortning för Wireless fidelity utan en ordvits på Hi-Fi även om begreppets ursprung är omtvistat |
| WAN | Geografiskt stora datornätverk | Wide Area Network |
| WTSA | Kongress som anordnas av ITU vart fjärde år för att lägga fast riktlinjer för organisationens arbete | World Telecommunication Standardization Assembly |
| ZTE | Kinesiskt telekombolag | |

# Enheter och mått i rapporten

| | | |
|---|---|---|
| **Hertz, enhet för frekvens** | | |
| | MHz | $10^6$ Hz |
| | GHz | $10^9$ Hz |
| **Bit, enhet för mängd data/information** | | |
| | Mbit | $10^6$ bit |
| | Gbit | $10^9$ bit |
| | Tbit | $10^{12}$ bit |
| **Överföringshastighet** | | |
| | Mbit/s | $10^6$ bit/sekund |
| | Gbit/s | $10^9$ bit/sekund |
| | Tbit/s | $10^{12}$ bit/sekund |
| **Megawatt, effekt, mäter energiproduktion** | MW | $10^6$ watt |

ISSN 1650-1942

www.foi.se