DIGITAL EKONOMI

26 november 2024

ICC Sweden

Mötets öppnande

Rapport från ICC
Jesper Labardi, ICC Sverige
Rene Summer, Ericsson

Global Digital Compact
Linn Engvall, Utrikesdepartementet

UN Convention Against Cybercrime
Alexander Fassihi, Justitiedepartementet

Hur främjar vi små och medelstora företags implementering av AI?
Sara Övreby, Google Sverige
Axel Tandberg, Legal Works Advisory

Mötets avslut

Rapport från ICC

Jesper Labardi, ICC Sverige
Rene Summer, Ericsson

ICC Sweden

Ny ICC-rapport: Overarching Narrative on Artificial Intelligence

- Syftet med arbetet har varit att samla ICC:s övergripande position vad gäller styrningen av AI.
- Rapporten utgår från fyra pelare:
    1. Principer och uppförandekoder
    2. Reglering
    3. Tekniska standarder
    4. Självreglering
- Rapporten innehåller även konkreta företagsexempel om hur näringslivet bidrar till ansvarsfull AI.

Digitaliseringen av handelsdokument i Sverige

Rättslägesanalys
& 10 argument

Debattartikel

Hemställan

Rundabordssamtal med
Luca Castellani, UNCITRAL

Nästa möte i arbetsgruppen anordnas **den 26 november** där vi får besök av **Chris Southworth**, generalsekreterare ICC UK.

FÖR DISKUSSION:

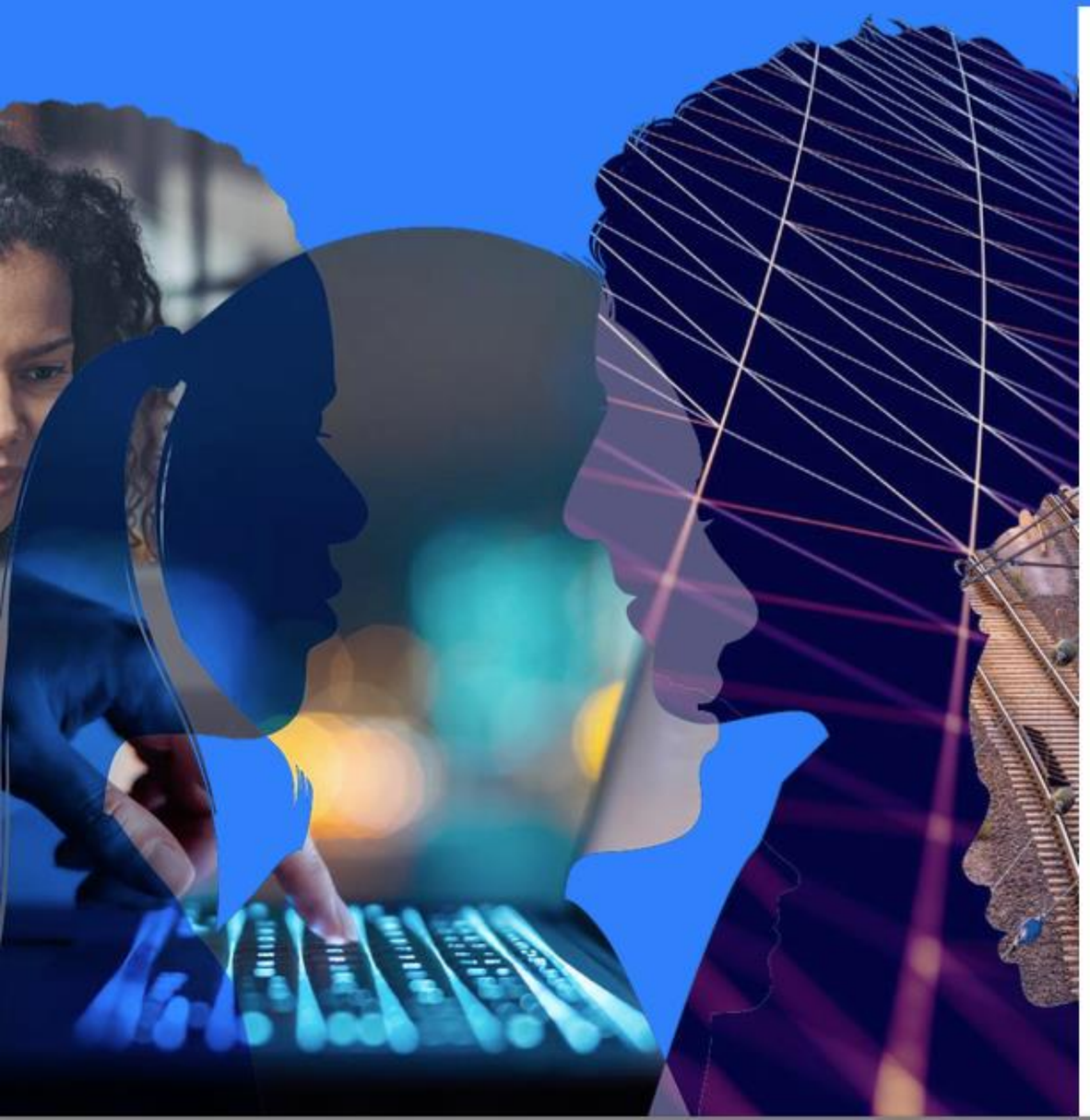
Globala prioriteringar 2025

- Advocate for stronger cybersecurity, enhanced international cooperation to combat cybercrime, and secure cross-border data flows to **help build a trusted and secure digital economy**.

- Inform the **development of global policy** frameworks to enable ”data free flow with trust”, focusing on the intersection of data and trade policies.

- Advocate for policy and governance frameworks that promote and enable **meaningful and inclusive access to existing and emerging technologies**, in particular artificial intelligence.

- **Lead business engagement in intergovernmental discussions** on the future governance of the internet, together with the ICC BASIS initiative.

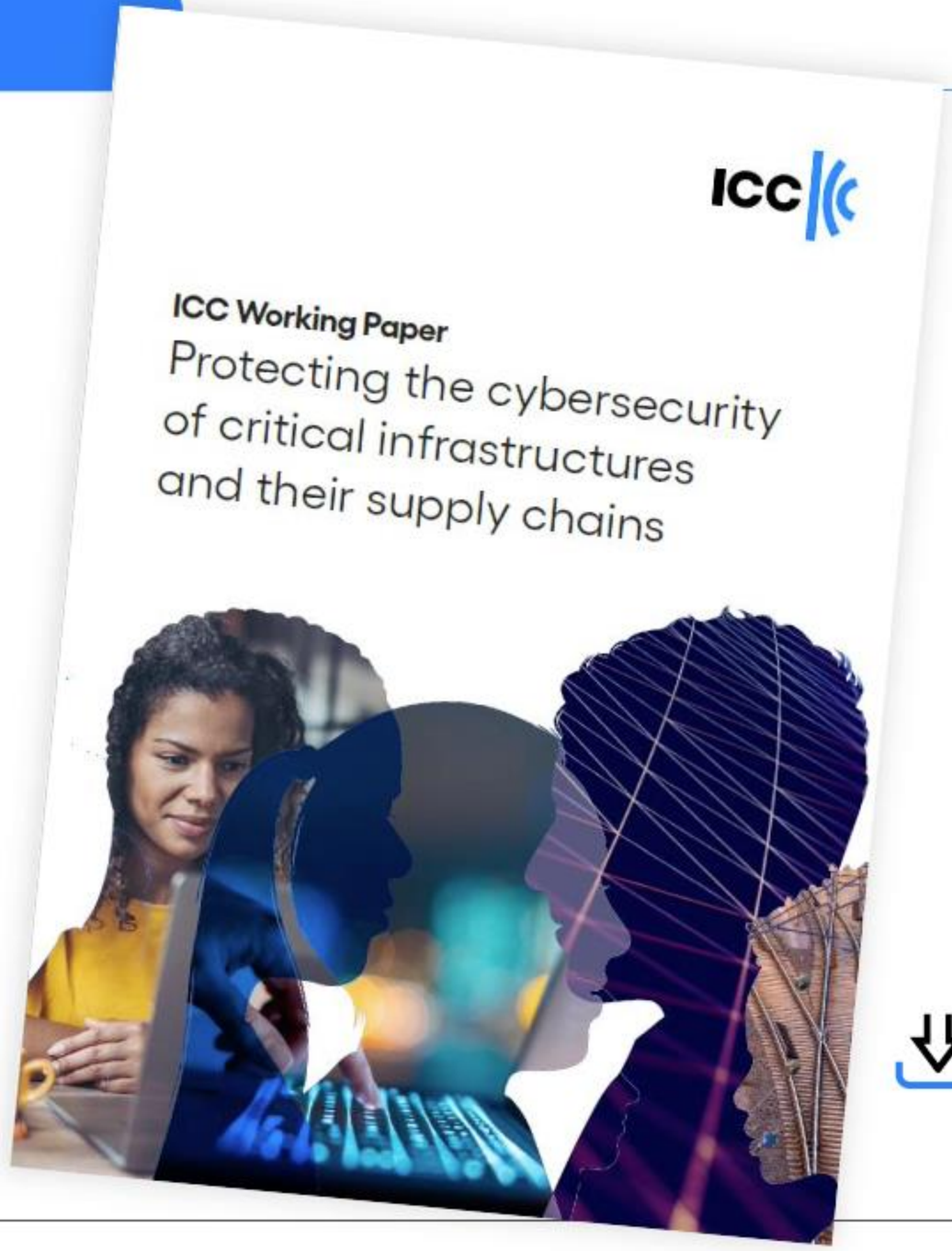


Working Paper

Protecting the cybersecurity of critical infrastructures and their supply chains

Content

1. **Background**
2. **Strategic objectives**
3. **Overview**
   - Dilemmas
   - Challenges
   - Current status
   - Path forward
   - Recommendations



Download
at iccwbo.org

What is at stake?

Disruptions affect

Public safety

Economic stability

National security

Motivation

- Increased national focus
- Sophisticated cyber threats
- Interconnectedness of CI
- Pressure on industry to increase resilience
  - → Growing compliance burdens
  - → Risk of fragmenting the global policy, legal and regulatory space

Purpose

1. address **cyber resilience measures**, including
   - collaboration mechanisms,
   - private sector voluntary measures
   - balance between regulation and the sustainability of controls.

2. call on **all stakeholders**, particularly governments, to fulfil their role

3. advocate for a **global holistic approach**

What is cyber resilience?

The ability of a critical entity to prevent, protect, respond, resist, mitigate, absorb, adapt and recover in the event of a cyber incident.

About the Working Paper

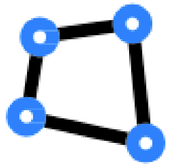
Objectives

Address
the multifaceted challenges of protection

Examine
diverse perspectives on defining CI

Identify
actors, motivations, and impacts of cyber threats

Underscore
the urgency of a harmonised approach



Call for
a relationship between CI providers, key supply chain stakeholders and governments

Assess
the current state of protection efforts and areas for improvement

Dilemmas

- Varying definitions across jurisdictions
- Combination of physical and digital elements increase vulnerability
- Interconnected global impacts and shared dependencies
- Complex supply chain risks
  - Increased exposure to risks
  - Lack of preparation and ability to respond

Actors, threats, response

Industry best practices

- comprehensive security measures
- robust asset inventories
- incident response plans
- strong data backups
- sound supply chain policy
- cybersecurity trainings

✓ providers need to build resilience and adopt best practices in risk management

Policy and regulatory approaches

- providers face constraints
- at national level, different regulations bring more generic frameworks and ease further compliance check by regulatory bodies

✓ appropriate mapping of regulations across geographies and sectors of activity is required

Industry best practices

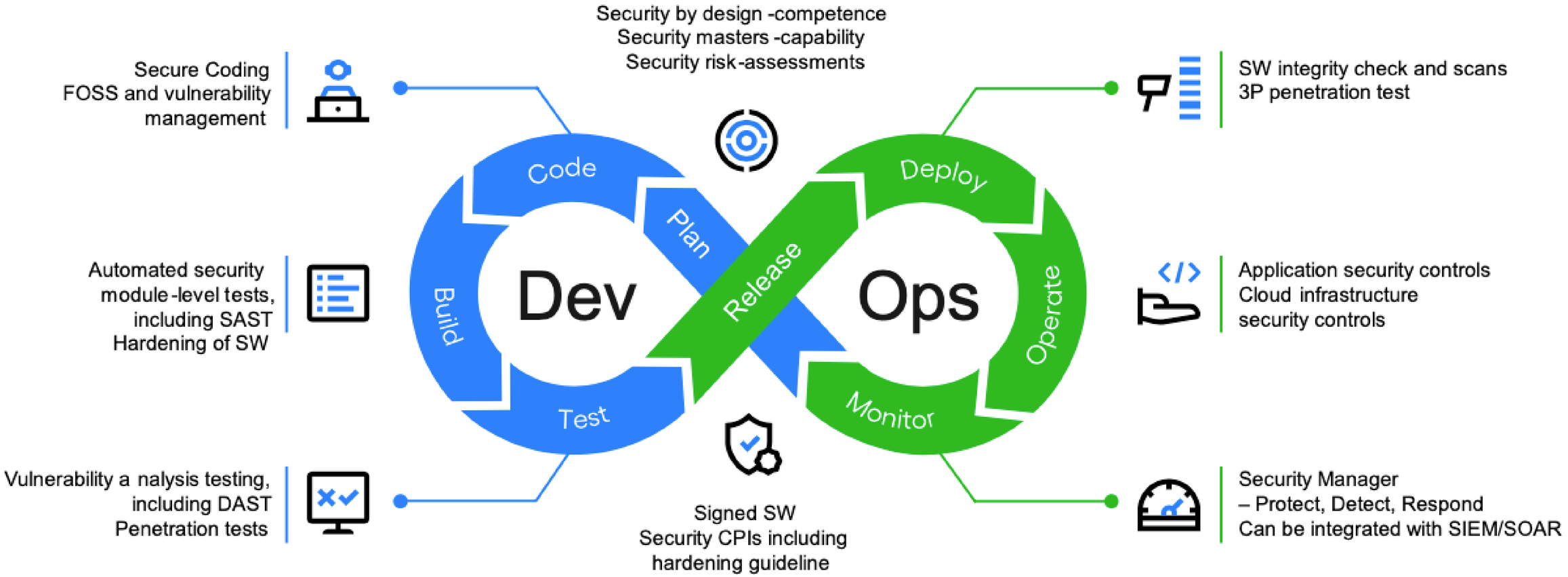
- Focus on a set of priority security requirements
- Reduce the impact of third-party incidents via discrete actions
- Partner with suppliers
- Leverage emerging technologies
- Add incentives and enforcements to contracts
- Establish processes to increase business leaders' involvement

Policy and regulatory approaches

- regulations and legislation to mandate secure software development practices
- diversification is key
- cooperative and coordinated approach is essential

Where are we now?

Securing the software supply chain



Source, Ericsson, Secure product development, based on Ericsson Security Reliability Model

What is needed

- **balanced, well-targeted and proportionate approach** for all CI and ES service providers
- **national and international regulatory framework** that enforces and incentivises appropriate behaviour
- **residual risks need to be mitigated** by measures aimed to decrease potential threats.

These measures involve

I. disrupting cyber threat actors
II. prosecuting cybercrimes more effectively
III. fostering urgent, large-scale, and effective implementation of the widely agreed existing norms and rules for state behaviour in cyberspace by setting shared goals for action

Essential first steps

- **Harmonise** efforts to set a baseline
- **Find** common agreement on terminology
- **Use** international standards
- **Adopt** strong third-party risk management approaches
- **Foster** transnational agreements
- **Decrease** cyber threats
- **Identify** incentives and deterrents for cybersecurity investment

Recommendations

Private sector

Implement cybersecurity frameworks

Regularly update and back up data

Patch vulnerabilities

Employ multifactor authentication

Develop detailed incident response plans

Conduct training and crisis drills

Monitor potential risks from suppliers

Recommendations

Policymakers

Establish independent cybersecurity agencies

Develop holistic, coordinated national cybersecurity policies

Create clear legislative frameworks with well-defined roles across government bodies

Collaborate with the private sector to develop national security plans and ensure transparency in designating critical assets

Strengthen supply chain protection through international standards

International cooperation

Harmonise regulatory approaches

Coordinate cybersecurity efforts globally

Advocate for new international norms against state-sponsored cyberattacks

Issue public attributions following incidents

Implement robust deterrent measures for cyberattacks

Promote international cooperation through diplomatic forums and structured multistakeholder engagement

Public-private partnerships

Integrate cybersecurity investment into national development plans and provide financial incentives for private sector compliance;

Encourage innovation in cybersecurity through funding and support for technology development, including AI;

Foster a culture of cybersecurity by promoting information sharing and enhancing cybersecurity capacity across all sectors;

Mandate cybersecurity requirements in government procurement and increase support for information sharing and analysis centers.

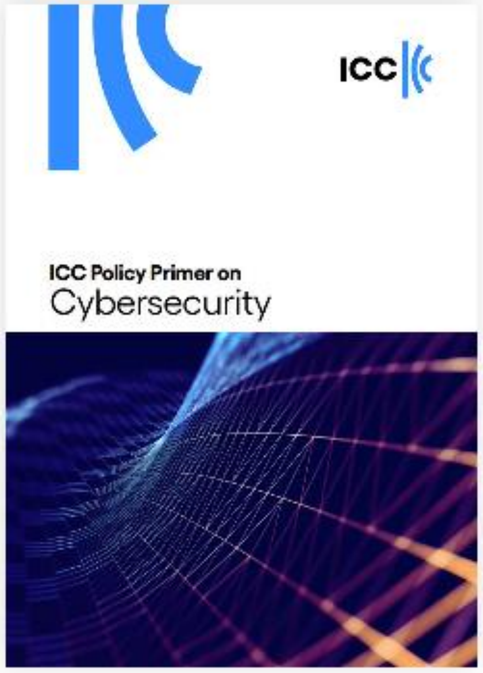
Find out more

Download

ICC Working Paper on
Protecting the cybersecurity of critical infrastructures and their supply chains

Read
the other papers from the ICC Cybersecurity issue brief series:

- ICC Policy Primer on Cybersecurity
- ICC Cybersecurity Issue Brief #1: Call for government action on cybersecurity
- ICC Cybersecurity Issue Brief #2: Implementing norms and rules for responsible state behaviour in cyberspace and enhancing cooperation to counter cybercrime



Global Digital Compact

Linn Engvall, Utrikesdepartementet

ICC Sweden

Det globala digitala ramverket (GDC)

Regeringskansliet

Vägen till Framtidstoppmötet och GDC

- Vid FN:s 75-årsfirande 2020 antogs en deklaration för stärkt multilateralt samarbete och med ett uppdrag åt generalsekreteraren

- Our Common Agenda-rapporten från 2021

- Förhandlingar inför Framtidstoppmötet

Regeringskansliet

Framtidspakten

Fem tematiska kapitel:

- Utveckling och utvecklingsfinansiering
- Internationell fred och säkerhet
- Forskning, innovation, teknologi
- Unga och framtida generationer
- Multilaterala styrningsformer

Annex

- Deklaration om unga och framtida generationer
- Det globala digitala ramverket (GDC)

UNITED NATIONS SECRETARY-GENERAL
ANTÓNIO GUTERRES

"Digital technology is shaping history. But there is also the sense that it is running away with us. Where will it take us? Will our dignity and rights be enhanced or diminished? Will our societies become more equal or less equal? Will we become more, or less, secure and safe? The answers to these questions depend on our ability to work together across disciplines and actors, across nations and political divides. We have a collective responsibility to give direction to these technologies so that we maximize benefits and curtail unintended consequences and malicious use."

Antagandet av GDC

- Världens första heltäckande globala digitala ramverk, antogs med konsensus av alla FN:s medlemsländer
- Åtaganden om hur vi vill att nuvarande och framväxande teknologier ska hanteras och styras
- Sverige och Zambia har lett förhandlingarna
- Omfattande konsultationsprocess för att säkerställa bred uppsättning perspektiv från experter, privat sektor, civilsamhället, m.fl.
- Gick i mål vid antagandet av Framtidspakten vid Framtidstoppmötet

United Nations

Global Digital Compact

An open, safe and secure digital future for all.

Global Digital Compact

A comprehensive framework for global governance of digital technology and artificial intelligence

GDC

- 13 övergripande principer
- Fem målsättningar:

- Slut digitala klyftor, påskynda genomförandet av Agenda 2030
- Öka inkludering i och fördelar av den digitala ekonomin
- Främja ett inkluderande, öppet, säkert digitalt system med respekt för MR
- Utveckla ansvarsfulla, kompatibla förhållningssätt till datahantering
- Förbättra den internationella styrningen av AI med människan i centrum

Slut digitala klyftor, påskynda Agenda 2030, öka inkludering i digitala ekonomin

- Öka det internationella samarbetet
- Tekniköverföring och kapacitetsuppbyggnadsinsatser på frivillig basis
- Öka den globala uppkopplingen – tillgång till globala marknader, främjar tillväxt och jobbskapande

Regeringskansliet

Främja ett inkluderande, öppet, säkert digitalt system med respekt för MR

- Informationsintegritet
- Motverka nätmobbing, exploatering och övergrepp
- Motståndskraftiga informationssystem
- Yttrandefrihet
- Digitala plattformar – innehållsmoderering, rapporteringsmekanismer

Förbättra den internationella styrningen av AI med människan i centrum

- Internationellt samarbete och en bred ”multiaktörsansats”
- AI-styrning grundad i folkrätten med människan i centrum
- Tre AI-specifika initiativ i ramverket:

- Global dialog om AI-styrning
- AI-expertpanel
- AI-kapacitetsuppbyggnad

Regeringskansliet

Ramverkets genomförande – vad händer nu?

- Brett ägarskap för uppföljningen, inkl. från privat sektor
- Endossering av ramverket görs på hemsidan
- Uppföljning i många parallella processer
- Nytt samordningskontor för digitala frågor på FN-sekretariatet
- Internet Governance Forum, ITU, WSIS+20
- Genomförandeplan presenteras i Q1 2025
- Uppföljningsmöte i FN:s generalförsamling 2027

Regeringskansliet

UN Convention Against Cybercrime

Alexander Fassihi, Justitiedepartementet

ICC Sweden

FN:s cyberbrottskonvention

26 november 2024 – ICC Sveriges kommitté för digital ekonomi

Alexander Fassihi

Rättssakkunnig vid Enheten för brottmålsärenden och internationellt rättsligt samarbete (BIRS), Justitiedepartementet

Bakgrund - cyberbrott

- Datorer och internets påverkan på brottsligheten
- Väl fungerande internationellt samarbete krävs
- Europarådets konvention om it-relaterad brottslighet (Budapestkonventionen)

Förhandlingarna av FN:s cyberbrotts-konvention

- AHC: Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

- Etablerades genom resolution 74/247 den 27 december 2019 och arbetsupplägget bestämdes i resolution 75/282 den 26 maj 2021

- Sex förhandlingssessioner och en avslutande förhandlingssession (som förlängdes) år 2022-2024

Sveriges position i förhandlingarna

- Förhandlingsmandat till EU-kommissionen från EU:s medlemsstater (rådets beslut 2022/895 av den 24 maj 2022) med förhandlingsdirektiv

- Nationell ståndpunkt i linje med detta:

- effektiv brottsbekämpning med starkt skydd för mänskliga rättigheter,

- kompatibel med befintliga internationella och regionala regelverk,

- tydliga och precisa bestämmelser

Förhandlingarnas dynamik

- Svåra förhandlingar givet frågan och omvärldsläget

- Skiljelinjer i fråga om:

- skyddet för mänskliga rättigheter

- konventionens omfattning: terminologi, kriminaliseringar, internationellt samarbete

- ikraftträdande och protokoll

- sexualbrotten

Förhandlingarnas avslutning

- Texten till konventionen antogs av AHC den 8 augusti 2024 (efter viss omröstning)

- Konventionen förväntas antas av FN:s generalförsamling i december 2024

Konventionens innehåll

Inspiration från:

- Budapestkonventionen
- UNTOC (FN:s konvention mot gränsöverskridande organiserad brottslighet)
- UNCAC (FN:s konvention mot korruption)

Titel

United Nations convention against cybercrime; Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes

Struktur

- Preamble
- Chapter I – General provisions
- Chapter II – Criminalization
- Chapter III – Jurisdiction
- Chapter IV – Procedural measures and law enforcement
- Chapter V – International cooperation
- Chapter VI – Preventive measures
- Chapter VII – Technical assistance and information exchange
- Chapter VIII – Mechanism of implementation
- Chapter IX – Final provisions
- Interpretative notes on specific articles

Kapitel 1 – General provisions

- **Article 1 – Statement of purpose**
- Article 2 – Use of terms
- Article 3 – Scope of application
- Article 4 – Offences established in accordance with other United Nations conventions and protocols
- Article 5 – Protection of sovereignty
- **Article 6 – Respect for human rights**

Artikel 1 – Statement of purpose

The purposes of this Convention are to:

a) Promote and strengthen measures to **prevent and combat cybercrime** more efficiently and effectively;

b) Promote, facilitate and strengthen **international cooperation** in preventing and comabting cybercrime; and

c) Promote, facilitate and support **technical assistance** and capacity-building to prevent and combat cybercrime, in particular for the benefit of developing countries.

Artikel 6 – Respect for human rights

1. Stats Parties shall ensure that the implementation of their obligations under this Convention is consistent with their obligations under international human rights law.
2. **Nothing in this Convention shall be interpreted as permitting** suppression of human rights or fundamental freedoms, including the rights related to the freedoms of expression, conscience, opinion, religion or belief, peaceful assembly and association, in accordance and in a manner consistent with applicable international human rights law.

Ingen motsvarighet i Budapestkonventionen, UNTOC eller UNCAC

Kapitel 2 – Criminalization

- Article 7 – Illegal access
- Article 8 – Illegal interception
- Article 9 – Interference with electronic data
- Article 10 – Interference with an information and communications technology system
- Article 11 – Misuse of devices
- Article 12 – Information and communications technology system-related forgery
- Article 13 – Information and communications technology system-related theft or fraud
- **Article 14 – Offences related to online child sexual abuse or child sexual explotation material**
- **Article 15 – Solicitation or grooming for the purposes of committing a sexual offence against a child**
- **Article 16 – Non-consensual dissemination of intimate images**

Kapitel 2 – Criminalization forts

- Article 17 – Laundering of proceeds of crime
- Article 18 – Liability of legal persons
- Article 19 – Participation and attempt
- Article 20 – Statute of limitations
- Article 21 – Prosecution, adjudication and sanctions

Kapitel 3 – Jurisdiction

- Article 22 – Jurisdiction

Kapitel 4 – Procedural measures and law enforcement

- Article 23 – Scope of procedural measures
- **Article 24 – Conditions and safeguards**
- Article 25 – Expedited preservation of stored electronic data
- Article 26 – Expedited preservation and partial disclosure of traffic data
- Article 27 – Production order
- Article 28 – Search and seizure of stored electronic data
- Article 29 – Real-time collection of traffic data
- Article 30 – Interception of content data
- Article 31 – Freezing, seizure and confiscation of the proceeds of crime
- Article 32 – Establishment of criminal record
- Article 33 – Protection of witnesses
- Article 34 – Assistance to and protection of victims

Artikel 24 – Conditions and safeguards

1. Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this chapter are subject to conditions and safeguards provided for under its domestic law, which shall provide for the protection of human rights, in accordance with its obligations under international human rights law, and which shall incorporate **the principle of proportionality**.
2. In accordance with and pursuant to the domestic law of each State Party, such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, include, inter alia, **judicial or other independent review, the right to an effective remedy, grounds justifying application, and limitation of the scope and the duration of such power or procedure**.

Artikel 24 – Conditions and safeguards forts

3. To the extent that it is consistent with the public interest, in particular the proper administration of justice, each State Party shall consider the impact of the powers and procedures in this chapter upon **the rights, responsibilities and legitimate interests of third parties**.
4. The conditions and safeguards established in acccordance with this article shall apply at the domestic level to the powers and procedures set forth in this chapter, **both** for the purpose of domestic criminal investigations and proceedings and for the purpose of rendering international cooperation by the requested State Party.
5. References to judicial or other independent review in paragraph 2 of this article are references to such review at the domestic level.

Jfr. artikel 15 i Budapestkonventionen

Kapitel 5 – International cooperation

- Article 35 – General principles of international cooperation
- **Article 36 – Protection of personal data**
- Article 37 – Extradition
- Article 38 – Transfer of sentenced persons
- Article 39 – Transfer of criminal proceedings
- Article 40 – General principles and procedures relating to mutual legal assistance
- Article 41 – 24/7 network
- Article 42 – International cooperation for the purpose of expedited preservation of stored electronic data
- Article 43 – International cooperation for the purpose of expedited disclosure of preserved traffic data

Kapitel 5 – International cooperation forts

- Article 44 – Mutual legal assistance in accessing stored electronic data
- Article 45 – Mutual legal assistance in the real-time collection of traffic data
- Article 46 – Mutual legal assistance in the interception of content data
- Article 47 – Law enforcement cooperation
- Article 48 – Joint investigations
- Article 49 – Mechanisms for the recovery of property through international cooperation in confiscation
- Article 50 – International cooperation for the purposes of confiscation
- Article 51 – Special cooperation
- Article 52 – Return and disposal of confiscated proceeds of crime or property

Artikel 36 – Protection of personal data

1. (a) A State Party transferring personal data pursuant to this Convention shall do so in accordance with its domestic law and any obligations the transferring Party may have under applicable international law. States Parties shall not be required to transfer personal data in accordance with this Convention if the data cannot be provided in compliance with their applicable laws concerning the protection of personal data;

(b) Where the transfer of personal data would not be compliant with paragraph 1 (a) of this article, States Parties may seek to impose appropriate conditions, in accordance with such applicable laws, to achieve compliance in order to respond to a request for personal data;

(c) States Parties are encouraged to establish bilateral or multilateral arrangements to facilitate the transfer of personal data.

Artikel 36 – Protection of personal data forts.

2. For personal data transferred in accordance with this Convention, States Parties shall ensure that the personal data received are subject to effective and appropriate safeguards in the respective legal frameworks of the States Parties.

3. In order to transfer personal data obtained in accordance with this Convention to a third country or an international organization, a State Party shall notify the original transferring State Party of its intention and request its authorization. The State Party shall transfer such personal data only with the authorization of the original transferring State Party, which may require that the authorization be provided in written form.

Kapitel 6 – Preventive measures

- Article 53 – Preventive measures

Kapitel 7 – Technical assistance and information exchange

- Article 54 – Technical assistance and capacity-building
- Article 55 – Exchange of information
- Article 56 – Implementation of the Convention through economic development and technical assistance

Kapitel 8 – Mechanism of implementation

- **Article 57 – Conference of the States Parties to the Convention**
- Article 58 – Secretariat

Artikel 57 – Conference of States Parties

1. A Conference of the States Parties to the Convention is hereby established to improve the capacity of and cooperation between the States Parties to achieve the objectives set forth in this Convention and to promote and review its implementation.

[…]

5. The Conference of the States Parties shall agree upon activities, procedures and methods of work to achieve the objectives set forth in paragraph 1 of this article, including:

[…]

(b) Facilitating the exchange of information on legal, policy and technological developments pertaining to the offences established in accordance with this Convention and the collection of evidence in electronic form among States Parties and relevant international and regional organizations, as well as non-governmental organizations, civil society organizations, academic institutions and **private sector entities**, in accordance with domestic law, as well as on patterns and trends in cybercrime and on successful practices for preventing and combating such offences;

Artikel 57 – Conference of States Parties forts

(c) Cooperating with relevant international and regional organizations, as well as non-governmental organizations, civil society organizations, academic institutions and **private sector entities**;

[…]

6. Each State Party shall provide the Conference of States Parties with information on legislative, administrative and other measures, as well as on its programmes, plans and practices, to implement this Convention, as required by the Conference. The Conference shall examine the most effective way of receiving and acting upon informatio, including, inter alia, information received from States Parties and from competent international and regional organizations. Inputs received from representatives of relevant non-governmental organizations, civil society organizations, academic institutions and **private sector entities**, duly accredited in accordance with procedures to be decided upon by the Conference, may also be considered.

Kapitel 9 – Final provisions

- Article 59 – Implementation of the Convention
- Article 60 – Effects of the Convention
- Article 61 – Relation with protocols
- Article 62 – Adoption of supplementary protocols
- Article 63 – Settlement of disputes
- Article 64 – Signature, ratification, acceptance, approval and accession
- **Article 65 – Entry into force**
- Article 66 – Amendment
- Article 67 – Denunciation
- Article 68 – Depositary and languages

Artikel 65 – Entry into force

1. This Convention shall enter into force on the ninetieth day after the date of deposit of the **fortieth [40] instrument of ratification**, acceptance, approval or accession. For the purpose of this paragraph, any instrument deposited by a regional economic integration organization shall not be counted as additional to those deposited by member States of that organizaton.

[…]

Skyddet för mänskliga rättigheter – omröstningar begärda av Iran

Omröstningar begärda av Iran att ta bort följande bestämmelser:

- Artikel 6.2 (Respect for human rights)

- ”without right” i artikel 14.1 och artikel 14.3 (Offences related to online child sexual abuse or child sexual exploitation material)

- ”without right” i artikel 16 och artikel 16.3 (Non-consensual dissemination of intimate images)

- Artikel 24 (Conditions and safeguards)

- Artikel 40.22 (General principles and procedures relating to mutual legal assistance)

Skyddet för mänskliga rättigheter – paket av bestämmelser

- Artikel 6 (Respect for human rights)
- Artikel 21.4 (Prosecution, adjudication and sanctions)
- Artikel 24 (Conditions and safeguards)
- Artikel 36 (Protection of personal data)
- En snävt och tydligt definierad omfattning på konventionen
- Kravet på dubbel straffbarhet
- Icke-diskrimineringsbestämmelse
- Hänvisningar till nationell rätt
- Avslagsgrunder

Vägen framåt

- Konventionen förväntas antas av FN:s generalförsamling i december 2024 och öppnas därefter för undertecknande och ratificering

- För detta krävs ett beslut från EU för Sveriges del

- Analys pågår

Hur främjar vi små och medelstora företags implementering av AI?

Sara Övreby, Google Sverige
Axel Tandberg, Legal Works Advisory

ICC Sweden

Nästa möte och avslut

ICC Sweden