

Effektiva ingripanden mot brott i cybermiljö



Brottsligheten har förändrats

- Ökad digitalisering och den tekniska utvecklingen spelar de kriminella i händerna (kryptering, anonymitet)
- De flesta brott har i dag någon digital komponent
- Polisiära ingripanden i den fysiska miljön är noga reglerade
- I cybermiljön saknas motsvarande reglering



Behovet av nya verktyg

- Cyberbrottslighet kräver ny reglering
- Effektiva och tidiga ingripanden behövs
- Regleringen måste innehålla starkt integritetsskydd
- En ny lag om polisiära ingripanden i cybermiljö föreslås



Den nya lagen

- Den nya lagen ska kunna användas av Polismyndigheten, Säkerhetspolisen och Tullverket
- Brotten ska helt eller delvis begås med hjälp av digitala informationssystem
- Brotten ska ha tydlig koppling till Sverige
- Brott med ett års fängelse i straffskalan
- Lagen ger myndigheterna rätt att vidta åtgärder som annars är kriminaliserade som dataintrång



Den nya lagen

- Ingripanden bör få beslutas om det är av **särskild vikt** för att
 - förhindra brott
 - avbryta brott
 - störa och avbryta brottslig verksamhet
 - kartlägga kommunikation till eller från ett informationssystem

Strängare krav ska gälla för radering än för andra ingripanden

Den nya lagen

- Bereda sig tillgång till uppgifter i informationssystem
- Byta lösenord och göra andra ändringar
- Blockera tillgång till uppgifter eller webbplats
- Tillfälligt ta kontroll över informationssystem
- Radera uppgifter

Exempel på brott

- Systematiska bedrägerier
- Narkotikaförsäljning online
- Olika brott som begås inom ramen för crime as a service
- Sexualbrott mot barn
- Terrorism
- Ransomwareangrepp
- Cyberspionage
- Spridning av skadlig programvara



Ikraftträdande m.m.

- Lagen tidsbegränsas till fem år
- Ikraftträdande föreslås den 1 juli 2027
- Gäller till utgången av juni 2032
- Utvärdering bör ske innan permanent reglering övervägs

