

Finansdepartementet  
103 33 Stockholm  
fi.remissvar@regeringskansliet.se

## Yttrande över Cyberresiliensutredningens betänkande 'Kompletterande bestämmelser till EU:s cyberresiliensförordning' (SOU 2025:115)

### Sammanfattning

Detta yttrande över innehållet i Cyberresiliensutredningens betänkande *Kompletterande bestämmelser till EU:s cyberresiliensförordning* (SOU 2025:115) redovisar ett antal synpunkter och rekommendationer utifrån en analys av innehållet i betänkandet (hädanefter refererat *betänkandet* i detta dokument). EU:s cyberresiliensförordning (eng. Cyber Resilience Act, hädanefter refererat *CRA* i detta dokument) trädde i kraft den 10 december 2024<sup>1</sup>. Rapporteringskrav börjar gälla från den 11 september 2026 och samtliga krav gäller från den 11 december 2027<sup>2</sup>.

Regeringens direktiv (Dir. 2024:119) uttrycker att en särskild utredare 'ska analysera behovet av och föreslå åtgärder och kompletterande författningsbestämmelser som behövs i syfte att anpassa svensk rätt till EU:s cyberresiliensförordning'. Av direktivet framgår att utredaren bland annat ska 'lämna de förslag, inklusive författningsförslag, i övrigt som är nödvändiga eller annars bedöms lämpliga för att komplettera förordningen'.

Utifrån en analys av regeringens direktiv<sup>3</sup> (Dir.2024:119), Cyberresiliensutredningens betänkande<sup>4</sup> (SOU 2025:115), den engelska språkversionen<sup>5</sup> av EU:s cyberresiliensförordning (hädanefter refererat *CRA-en*), den svenska språkversionen<sup>6</sup> av EU:s cyberresiliensförordning (hädanefter refererat *CRA-sv*), Europeiska kommissionens konsekvensbedömning av ett utkast till *CRA*<sup>7</sup>, Europeiska kommissionens uppdrag till tre standardiseringsorganisationer (CEN, Cenelec och ETSI) att utveckla standarder<sup>8</sup>, blir slutsatsen att det, i flera avseenden, finns brister i *CRA* som Cyberresiliensutredningen skulle kunna ha uppmärksammat på ett mer genomgripande sätt.

Detta yttrande fokuserar på ett *urval* aspekter som behandlats i Cyberresiliensutredningens betänkande, i (olika språkversioner av) *CRA*, samt i de standarder (from CEN, Cenelec och ETSI) och den vägledning (från EU) som växer fram med syftet att ge stöd för efterlevnad av *CRA*. Specifikt behandlar detta yttrande: 1) FOSS och annan typ av programvara; 2) FOSS-projekt; 3) Motsägelsefulla språkversioner av *CRA*; 4) Sekretess relaterat rapportering av sårbarheter; 5) Behov av ytterligare preciseringar och konsekvensbedömningar.

1 (EU, 2025e)

2 (EU, 2025e, 2025f)

3 (Regeringen, 2024)

4 (SOU, 2025)

5 (EU, 2024k)

6 (EU, 2024l)

7 (EU, 2022a, 2022b, 2022c, 2022d, 2022e)

8 (EU, 2025a, 2025b)

## Bakgrund

### **Om detta yttrande:**

Detta yttrande har utformats av professor Björn Lundell (Ph.D.) vid Högskolan i Skövde. De synpunkter och rekommendationer som framförs i detta yttrande baseras på erfarenheter och resultat från flera års forskning inom området för Cyberresiliensutredningens betänkande. Yttrandet ger uttryck för den enskilde forskarens egen uppfattning och ska därför inte uppfattas som ett ställningstagande från lärosätet (Högskolan i Skövde).

Ett urval källor redovisas i en källförteckning till detta yttrande. Källförteckningen inkluderar även ett antal källor som refererar tidigare lämnade yttranden och rapporter som författaren tidigare bidragit med, vilket inkluderar: rapporter från relaterade utredningar som professor Lundell genomfört och bidragit till på uppdrag av svenska myndigheter (specifikt Statens inköpscentral vid Kammarkollegiet<sup>9</sup>, Konkurrensverket<sup>10</sup> & Myndigheten för digital förvaltning: DIGG<sup>11</sup>); yttranden till relaterade utredningar som genomförts i Sverige (däribland till: SOU 2021:1<sup>12</sup>, Riksarkivets författningsförslag<sup>13</sup>, SOU 2021:97<sup>14</sup> & SOU 2025:12<sup>15</sup>); samt yttranden till öppna konsultationer som genomförs inom EU (specifikt relaterat: analyser av programvarusystem (som identifierat allvarliga brister i ENISA's utkast<sup>16</sup> till SBOMs<sup>17</sup>), offentlig upphandling<sup>18</sup>, standardisering<sup>19</sup> och patent som belastar standarder<sup>20</sup>, s.k. SEPs).

Dessutom har professor Lundell, såväl inom Sverige<sup>21</sup> och inom EU<sup>22</sup>, bidragit med yttranden över innehållet i lagförslag till CRA.

### **Om författaren till detta yttrande:**

Författaren till detta yttrande (*nedan författaren*) heter Björn Lundell och är professor i datavetenskap vid Högskolan i Skövde där han leder forskningen inom Software Systems Research Group (SSRG). Under lång tid har författaren, tillsammans med kollegor och flera samverkanspartners, genomfört forskning som behandlat flera frågeställningar som i högsta grad berör AI-kommissionens betänkande. Detta inkluderar studier som genomförts inom ramen för olika uppdrag i samverkan med svenska myndigheter, däribland Statens inköpscentral vid Kammarkollegiet, Konkurrensverket och Myndigheten för digital förvaltning (DIGG).

Inom ramen för ett stort antal internationella och nationella forskningsprojekt har författaren, tillsammans med kollegor och samverkanspartners, genomfört ett stort antal studier som behandlat en rad (tekniska, socio-tekniska, juridiska och samhällsrelaterade) frågeställningar avseende hur olika intressenter (enskilda individer, företag, offentliga organisationer, nationer och EU) styr (genom lagstiftning, föreskrifter, policy, rekommendationer, etc.) samt i praktiken agerar då

---

9 (NPS, 2016)

10 (Lundell et al., 2016)

11 (Lundell, 2020)

12 (Lundell, 2021)

13 (Lundell, 2022a)

14 (Lundell, 2022b)

15 (Lundell, 2025a)

16 (Georgiadou et al., 2025)

17 (Lundell, 2026a)

18 (Lundell, 2026b)

19 (Lundell, 2025b)

20 (EU, 2014; Lundell, 2022c, 2023)

21 (Lundell, 2023b, 2023c)

22 (Lundell, 2024a, 2024b)

programvarusystem anskaffas, utvecklas, förvaltas och används. De studier som genomförts inom ramen för denna forskning har haft betydande inverkan på kunskapsutvecklingen inom området och samhället i stort.

Den forskning som SSRG bedriver har under flera decennier fokuserat på tre övergripande forskningsutmaningar: inlåsnings effekter, interoperabilitet samt långa livscykler för system och relaterade digitala tillgångar (eng. 'digital assets'). Forskningen har (länge) haft betydande fokus på förutsättningar för utveckling och användning av standarder och FOSS<sup>23</sup> (Free and Open Source Software), samt frågeställningar avseende under vilka villkor olika typer av IKT-standarder kan implementeras av programvaruprojekt som utvecklar och tillhandahåller FOSS. Exempelvis genomförde författaren till detta yttrande flera analyser av industriföretags engagemang med FOSS under genomförandet av EU FP6-projektet Calibre (2004-2006). Därefter har författaren, tillsammans med kollegor och samverkanspartners, genomfört omfattande forskning inom ramen för flera internationella (däribland EU-projekten COSI och OPEES) och nationella forskningsprojekt (däribland LIM-IT och SUDO).

Genomförd forskning har regelbundet publicerats i relevanta vetenskapliga fora och i flera fall dessutom kommunicerats till det omgivande samhället genom nyheter, konferenser (exempelvis genom den årligen återkommande konferensen Hållbar digitalisering<sup>24</sup> som arrangerats sedan 2019 och andra internationella<sup>25</sup> och nationella konferenser som genomförts med olika fokus) och öppna seminarier som riktar sig till det omgivande samhället. Vetenskapligt granskade resultat från denna forskning har publicerats och presenterats i en rad olika fora. Flera genomförda studier inkluderar rekommendationer för hur företag, myndigheter och samhället i stort kan (och bör) strategiskt engagera sig med upphandling, utveckling och it-drift av programvarusystem, specifikt relaterat: anskaffning och användning av molntjänster, engagemang med FOSS-projekt och IKT-standarder, samt FOSS-projekts användning och implementation av IKT-standarder.

---

23 FOSS (Free and Open Source Software) är en delmängd av all programvara. FOSS (på svenska 'fri och öppen programvara') är programvara som tillhandahålls under villkor och licenser som uppfyller definitionen 'the Free Software Definition' (FSD, 2026) och som uppfyller definitionen 'the Open Source Definition' (OSD, 2026), se vidare Lundell (2020). Definitionen av fri programvara (FSD, 2026) har etablerats av organisationen Free Software Foundation (FSF, 2026) och definitionen av öppen programvara (på svenska ibland även benämnt 'öppen källkod') har etablerats av organisationen Open Source Initiative (OSI, 2026). Fri programvara (på engelska 'Free Software', vanligen förkortat 'FS') är programvara som tillhandahålls under villkor och licenser som uppfyller 'the Free Software Definition' (FSD, 2026). Öppen programvara (på engelska 'Open Source Software', vanligen förkortat OSS) är programvara som tillhandahålls under villkor och licenser som uppfyller 'the Open Source Definition' (OSD, 2026). FOSS har länge använts av forskare som en inkluderande term för FS (Free Software) och OSS (Open Source Software) och under 2024 antog EU förordningen om cyberresiliens (Cyber Resilience Act, CRA) som påverkar förutsättningarna för all programvara och det finns särskilda regler som påverkar förutsättningarna för FOSS (EU, 2024k, 2024l).

24 För en översikt av de konferenser (Hållbar digitalisering) som genomförts under 2020, 2021, 2022, 2023 och 2024, se: <https://www.ssr.info/hd2020/>, <https://www.ssr.info/hd2021/>, <https://www.ssr.info/hd2022/>, <https://www.ssr.info/hd2023/>, <https://www.ssr.info/hd2024/> och <https://www.ssr.info/hd2025/>

25 Exempelvis genomfördes konferensen 'Öppen programvara i en föränderlig värld: Hur upprätthålls och accelereras affärs- och samhälls effekter samtidigt som aktuella utmaningar hanteras?' (eng. 'Open Source in a changing world: How to sustain and accelerate business and societal impact while navigating contemporary challenges?') med flera internationella experter den 16 april 2024, <https://www.ssr.info/oppen-programvara-i-en-foranderlig-varld/>. Under denna konferens (och en relaterad workshop som genomfördes den 15 april 2024) behandlades flera aktuella frågeställningar avseende FOSS under flera paneldiskussioner, en posterutställning och fyra inbjudna presentationer som gavs av internationella experter. Exempelvis behandlades: FOSS i relation till AI-utvecklingen (av Pamela Chestek, [https://www.ssr.info/oppen-programvara-i-en-foranderlig-varld\\_chestek/](https://www.ssr.info/oppen-programvara-i-en-foranderlig-varld_chestek/)), FOSS i relation till standardisering (av Jorge L. Contreras, [https://www.ssr.info/oppen-programvara-i-en-foranderlig-varld\\_contreras/](https://www.ssr.info/oppen-programvara-i-en-foranderlig-varld_contreras/)), FOSS i relation till kommande EU-regelverk (av Mirko Boehm, [https://www.ssr.info/oppen-programvara-i-en-foranderlig-varld\\_boehm/](https://www.ssr.info/oppen-programvara-i-en-foranderlig-varld_boehm/)), samt exempel på möjligheter med molnbaserad FOSS med AI-funktionalitet som tillhandahålls och används i flera EU-länder (av Jos Poortvliet, [https://www.ssr.info/oppen-programvara-i-en-foranderlig-varld\\_poortvliet/](https://www.ssr.info/oppen-programvara-i-en-foranderlig-varld_poortvliet/)).

## FOSS och annan typ av programvara

Som nämns i den svenska språkversionen av EU:s blåbok<sup>26</sup> är programvara 'en nödvändig del av ett stort antal produkter'. Utifrån olika syften och incitament kan ett programvaruprojekt utveckla och tillhandahålla programvara. Programvara kan tillhandahållas på en marknad för användning av en lång rad intressenter och under många år har det varit vanligt att en specifik instans av en programvara tillhandahålls som 'programvaruprodukt'.

Utifrån ett uppdrag av Europeiska kommissionen<sup>27</sup> är tre Europeiska standardiseringsorganisationer (CEN, Cenelec och ETSI) engagerade med utveckling och tillhandahållande av standarder som organisationer kommer att kunna använda för att visa efterlevnad av CRA. Huruvida utvecklingen av dessa standarder kommer att kunna slutföras inom de givna tidsramar som EU preciserat och huruvida utvecklingen kommer att resultera i standarder med ändamålsenlig kvalitet är i skrivande stund en öppen fråga. Det kan noteras att intressenter under processen har uttryckt farhågor avseende förutsättningarna för att kunna utveckla och tillhandahålla standarderna<sup>28</sup>.

Det är en brist att *betänkandet* saknar en redovisning från någon analys av hur olika intressenter i Sverige kan komma påverkas av hur CRA påverkar förutsättningarna för olika intressenters fortsatta engagemang med utveckling, tillhandahållande och användning av programvara som tillhandahålls under olika villkor inom Sverige, inom EU och globalt.

Nästan all programvara inkluderar, helt eller delvis, programvara som tillhandahålls under villkor och licenser som uppfyller definitionen<sup>29</sup> av fri programvara<sup>30</sup> (eng. 'Free Software', vanligen förkortat 'FS') och uppfyller definitionen<sup>31</sup> av öppen programvara<sup>32</sup> (eng. 'Open Source Software', vanligen förkortat 'OSS'). FOSS (på svenska 'fri och öppen programvara') har länge<sup>33</sup> använts av forskare som en inkluderande term för programvara som tillhandahålls under villkor och licenser som uppfyller definitionen av fri programvara (Free Software) och uppfyller definitionen av öppen programvara (Open Source Software). FOSS är en delmängd av all programvara<sup>34</sup>.

Det är en allvarlig brist att *betänkandet* inte uppmärksammat att den svenska språkversionen av CRA (CRA-sv) saknar en definition av FOSS ('fri och öppen programvara'). Det är också en brist att *betänkandet* inte uppmärksammat att den engelska språkversionen av CRA innehåller en definition

---

26 Se avsnittet 'Programvara' i sektion '2.1 Vilka produkter omfattas?' av den svenska språkversionen av blåboken (EU, 2022g).

27 (EU, 2025a, 2025b)

28 Bland forskare och representanter för olika organisationer som utvecklar och tillhandahåller programvara som behöver uppfylla CRA har det uttryckts en oro för att arbetet kommer bli försenat och en frustration avseende under vilka förutsättningar och villkor arbetet bedrivs. Exempelvis har en forskare uttryckt följande: 'It is questionable whether flexible *ad hoc* collaboration forms are sufficient to structurally and consistently overcome risks of incoherence among the European standards developed by the ESOs in the area of cybersecurity resilience.' (Kamara, 2024)

29 'The Free Software Definition' (FSD, 2026). Definitionen av fri programvara (FSD, 2026) har etablerats av organisationen Free Software Foundation (FSF, 2026) och definitionen av öppen programvara (på svenska ibland även benämnt 'öppen källkod') har etablerats av organisationen Open Source Initiative (OSI, 2026). Organisationen Free Software Foundation (<https://www.fsf.org>) etablerades 1985 och organisationen Open Source Initiative (<https://opensource.org>) etablerades 1998.

30 Fri programvara (på engelska 'Free Software', vanligen förkortat 'FS') är programvara som tillhandahålls under villkor och licenser som uppfyller 'the Free Software Definition' (FSD, 2026)

31 'The Open Source Definition' (OSD, 2026). Definitionen av öppen programvara (på svenska ibland även benämnt 'öppen källkod') har etablerats av organisationen Open Source Initiative (OSI, 2026).

32 Öppen programvara (på engelska 'Open Source Software', vanligen förkortat 'OSS') är programvara som tillhandahålls under villkor och licenser som uppfyller 'the Open Source Definition' (OSD, 2026).

33 (González-Barahona, 2004)

34 (Lundell, 2020)

av FOSS (eng. 'Free and Open Source Software') som avviker från de, sedan länge, globalt erkända och etablerade definitionerna av FS, OSS och FOSS<sup>35</sup>.

Den engelska språkversionen av *CRA* (*CRA-en*) definierar 'open-source software steward' som en ny roll i *CRA*. I den svenska språkversionen (*CRA-sv*) definiera istället 'förvaltare av programvara med fri och öppen källkod' för denna roll. Det finns flera öppna frågor avseende vad denna nya roll i praktiken kommer att innebära för FOSS projekt<sup>36</sup>.

Att använda 'förvaltare' (som motsvarighet till 'steward') är olyckligt eftersom etablerad terminologi angående att förvalta FOSS är något annat än att agera i den roll som 'steward' innebär.

Det hade varit önskvärt att *betänkandet* föreslagit: (1) en revision av den svenska språkversionen av *CRA* (*CRA-sv*) avseende FOSS, samt (2) föreslagit att en vägledning ska utvecklas för att komplettera *CRA* avseende hur FOSS ska tolkas i en svensk kontext med syftet att reducera osäkerhet för alla individer och organisationer som direkt, eller indirekt, berörs av *CRA*.

Det finns en betydande risk att det uppstår osäkerhet avseende huruvida en specifik programvara utgör FOSS enligt *CRA*. Sådan osäkerhet riskerar orsaka en avkylande effekt hos enskilda individer och organisationer som är engagerade i olika programvaruprojekt. Detta riskerar, i sin tur, hämma förutsättningarna för upprätthållande av internationell samverkan och internationella affärer.

Under utvecklingen av *CRA* har många intressenter bidragit med synpunkter och kommentarer<sup>37</sup>, där flera uppmärksammat olika missförstånd avseende FOSS<sup>38</sup>. Förutsättningar för efterlevnad av *CRA* har behandlats<sup>39</sup>. Betydande missförstånd avseende FOSS och betydelsen av FOSS för många organisationer har uppmärksamrats under utvecklingen av *CRA*. Många företag är i dag beroende av, samt i många fall också direkt engagerade med, utveckling och tillhandahållande av FOSS. Flera brister och missförstånd avseende förutsättningarna för FOSS har påpekats under utvecklingen av *CRA*, inte minst när det gäller hur och under vilka förutsättningar olika typer av intressenter är engagerade med programvaruutvecklingsprojekt som utvecklar och tillhandahåller FOSS utifrån olika incitament.

---

35 (Lundell, 2020)

36 'While stewardship as a model of responsible governance has a vast and rich history, the reality is that it is a nascent concept for FOSS. With the EU's adoption of the landmark *CRA* and its novel regulatory category of 'FOSS stewards' – a world first – questions naturally have arisen of how it shall operate in practice, including possible implications for fairness, accountability and transparency.' (Tridgell & Singh, 2025)

37 (Brånby & Nilsson, 2025; Chiara, 2022; Colonna, 2025; Kikelj & Sabic, 2024; Lasota, 2025; Teichmann & Sergi, 2025; Teichmann, 2026; Tridgell & Singh, 2025)

38 'The initial version of the *CRA* drew sharp criticism from various entities, including over a dozen open-source industry bodies who wrote an open letter expressing concerns about its potential to stifle software development' (Colona, 2025)

39 Se exempelvis Teichmann (2026).

## FOSS-projekt

Europeiska kommissionens konsekvensbedömning<sup>40</sup> baseras på ett tidigt, mycket bristfälligt<sup>41</sup>, utkast till CRA. Detta tidiga utkast till CRA och konsekvensbedömningen genomsyras av flera missförstånd och direkta felaktigheter avseende FOSS<sup>42</sup>. Ett mycket allvarligt missförstånd är att det görs en distinktion mellan 'kommersiell' och 'icke-kommersiell' öppen programvara<sup>43</sup>. Denna distinktion baseras på ett missförstånd. Det finns ingen licens för öppen programvara som tillåter en sådan restriktion. Individer och organisationer kan utveckla och använda all öppen programvara utifrån en rad olika syften, men det finns ingen licens för öppen programvara som tillåter att programvaran endast kan användas för 'icke-kommersiella' syften. Som tidigare rapporterat till Finansdepartementet<sup>44</sup>, refererar konsekvensbedömningen<sup>45</sup> till en källa som inte ger stöd för lagförslagets argument till distinktion mellan 'kommersiell' och 'icke-kommersiell' öppen programvara. I den refererade källan saknas stöd för att beskriva öppen programvara som 'icke-kommersiell'.

Med hänvisning till den svenska språkversionen av Europeiska kommissionens blåbok<sup>46</sup> framgår av *betänkandet* att 'varje utbudande eller överlåtelse som kan leda till att en produkt övergår till en ny användare utgör ett tillhandahållande på marknaden'. Även om det i *betänkandet* finns en redogörelse för innebörden av 'tillhandahållande på marknaden' saknas ett resonemang om huruvida en specifik instans av programvara som tillhandahålls från ett programvaruprojekt utgör en produkt (d.v.s. en 'programvaruprodukt' som tillhandahålls på marknaden<sup>47</sup>, där produkten kan tillgängliggöras med eller utan kostnad under villkor som möjliggör att produkten kan användas av annan användare). Av den svenska språkversionen av blåboken<sup>48</sup> preciseras tillhandahållande på marknaden på följande sätt: '*En produkt tillhandahålls på marknaden när den levereras för distribution, förbrukning eller användning på unionsmarknaden i samband med kommersiell verksamhet, mot betalning eller gratis.*' Den engelska versionen av blåboken innehåller en likartad definition<sup>49</sup>. Vidare framgår av den svenska språkversionen av blåboken att 'Leverans av en produkt anses endast utgöra tillhandahållande på unionsmarknaden om produkten är avsedd för slutanvändning på unionsmarknaden'.

Innebörden av 'kommersiell verksamhet' är centralt för tolkningen av CRA och den svenska språkversionen av blåboken<sup>50</sup> innehåller följande precisering: 'Kommersiell verksamhet innebär tillhandahållande av varor i affärssammanhang. Icke-vinstdrivande organisationer kan anses bedriva kommersiell verksamhet om de är verksamma inom ett sådant sammanhang. Detta kan endast bedömas från fall till fall genom att ta hänsyn till leveransernas frekvens, produktens egenskaper,

---

40 (EU, 2022a, 2022b, 2022c, 2022d, 2022e)

41 (Lundell, 2023c)

42 (Lundell, 2023c)

43 (Lundell, 2023c)

44 (Lundell, 2023c)

45 I fotnot 16 av EC (2022c, s. 30) refereras Riehle (2009)

46 Specifikt hänvisas (på sidan 146 i *betänkandet*) till den svenska språkversionen av 'kommissionens vägledning' (EU, 2022g). På sidorna 146-147 i *betänkandet* finns en övergripande redogörelse för vad 'Tillhandahållande på marknaden' innebär.

47 Det är vanligt att FOSS-projekt som utvecklas i samverkan mellan olika intressenter successivt tillhandahåller specifika instanser av FOSS från projektet (d.v.s. som en FOSS-licensierad programvaruprodukt) och där en delmängd av dessa specifika instanser av FOSS genomgått en mer omfattande kvalitetsgranskning och då tillgängliggörs som en 'stabil release' (d.v.s. som en specifik instans av en FOSS-licensierad programvaruprodukt som kan tillhandahållas under olika villkor).

48 (EU, 2022g)

49 '*A product is made available on the market when supplied for distribution, consumption or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge.*' (EU, 2022f)

50 (EU, 2022g)

leverantörens avsikter osv. I princip bör enstaka leveranser av välgörenhetsorganisationer eller hobbyanvändare inte anses ske i affärssammanhang.’ För många intressenter är det mycket angeläget att det tillhandahålls preciserings- och ytterligare vägledning än det som redovisas i *betänkandet*.

Det hade varit önskvärt att *betänkandet*, på ett mer ingående sätt, redogjort för och preciserat vad CRA innebär för intressenter som – i olika roller – är engagerade med programvaruprojekt som tillhandahåller FOSS. Utveckling och tillhandahållande av FOSS (och annan programvara) kan ske på många sätt.

Genom åren har förutsättningarna för utveckling och tillhandahållande av programvara fundamentalt förändrats och redan för mer än 20 år sedan var det långt ifrån ovanligt att företag i Sverige engagerade sig med, samt bidrog till utveckling av, olika FOSS-projekt<sup>51</sup>. Fram till mitten av 1960-talet var det vanligt att användare utan kostnad delade programvaror<sup>52</sup>. Under 1960-talet var det en utbredd uppfattning att det saknas förutsättningar för kommersiellt tillhandahållande av programvara och det var vanligt att programvara tillhandahölls utan kostnad eller utvecklades specifikt för varje leverans av en dator<sup>53</sup>. Situationen förändrades 1969 när IBM tillkännagav att programvara skulle tillhandahållas kommersiellt frikopplat från tillhandahållande av datorer och under 1970-talet växte en marknad fram för kommersiellt tillhandahållande av programvara<sup>54</sup>.

Successivt har allt fler organisationer engagerat sig med FOSS och den ekonomiska betydelsen av FOSS är betydande<sup>55</sup>. Många företag engagerar sig med, samt bidrar strategiskt, till FOSS-projekt och många företag som påverkas av CRA är beroende av programvara är också beroende av FOSS<sup>56</sup>. Strategiska engagemang med FOSS-projekt ses i flera länder<sup>57</sup> också som en nödvändig (om än inte tillräcklig) förutsättning för att kunna etablera och upprätthålla digital suveränitet och full kontroll över behandling och förvaltning av nationers och enskilda organisationers digitala tillgångar.

Det är en brist att *betänkandet* i så hög utsträckning baseras på den mycket bristfälliga och icke relevanta konsekvensbedömningen<sup>58</sup>. Det hade varit önskvärt att *betänkandet* föreslagit att det genomförs en konsekvensbedömning som redovisar hur olika intressenter i Sverige kan komma påverkas av hur CRA.

---

51 (Lundell et al., 2006)

52 ‘In the earlier days of computing in the 1950s and the first half of the 1960s, software was considered to have a limited commercial value. Most computer manufacturers bundled software programs with their hardware at “no cost” and the community of users was willing to share the software programs and improvements they made.’ (Corrado et al., 2018).

53 ‘One cannot make any money selling software. That was the conventional wisdom in the 1960s, when software was either given away free by the computer manufacturer or written specifically and uniquely for each computer installation.’ (Johnson, 1998)

54 ‘The situation changed in 1969, when IBM announced the unbundling of software: part of its catalog was to be sold separately. From that moment on, users had to purchase some of the software they needed.’ (Gonzalez-Barahona, 2021)

55 (Blind et al., 2021)

56 (Lundell et al., 2022)

57 Ett exempel är Schleswig-Holstein som antaget en strategi för förbudsstaten (State Chancellery, 2024)

58 (EU, 2022a, 2022b, 2022c, 2022d, 2022e)

## Motsägelsefulla språkversioner av CRA

De 24 språkversioner av *CRA* som trädde i kraft den 10 december 2024 är motsägelsefulla och djupt problematiska avseende FOSS (fri och öppen programvara). Det är en brist att *betänkandet* inte uppmärksammat problem med motsägelsefulla språkversioner av en förordning<sup>59</sup>.

I *betänkandet* presenteras en bristfällig analys av hur *CRA* kan komma att påverka förutsättningarna för utveckling och användning av programvara under olika villkor. Detta gäller särskilt förutsättningar för programvaruprojekt som utvecklar och tillhandahåller FOSS<sup>60</sup>.

Den engelska språkversionen av *CRA* (*CRA-en*) inkluderar (i artikel 3 (48)) en definition av FOSS (som inleds med: '(48) 'free and open-source software' means ...'). Däremot saknas en definition av FOSS i svenska språkversionen av *CRA* (*CRA-sv*). Detta innebär att språkversionerna är motsägelsefulla.

Det är en allvarlig brist att *betänkandet* inte uppmärksammar och redovisar en analys av konsekvenser som kan bli följden av att den svenska språkversionen av *CRA* (*CRA-sv*) saknar en definition av FOSS.

Den svenska språkversionen av *CRA* (*CRA-sv*) inkluderar (i artikel 3 (48)) istället en definition (som inleds med: '48. *programvara med fri och öppen källkod*: programvara ...'). Inledningen på denna definition i den svenska språkversionen skulle kunna uppfattas som en definition av 'programvara med FOSS' (istället för en definition av 'FOSS').

Dessutom saknar frasen 'fri och öppen källkod' en definition i den svenska språkversionen av *CRA* (*CRA-sv*). Begreppen 'fri källkod' och 'öppen källkod' är också odefinierade i den svenska språkversionen. Dessutom är begreppet 'fri källkod' inte tidigare använt.

Det är mycket angeläget att korrigera den svenska språkversionen av *CRA* (*CRA-sv*) för att undvika problem då intressenter från olika länder samverkar.

Programvara som tillhandahålls under villkor och en licens som uppfyller FOSS (enligt definitionen av fri programvara<sup>61</sup> och enligt definitionen av öppen programvara<sup>62</sup>) är inte FOSS enligt flera av de 24 publicerade språkversionerna av *CRA*.

Programvara som tillhandahålls under villkor och en licens som uppfyller FOSS (enligt flera av de 24 publicerade språkversionerna av *CRA*) är inte FOSS (enligt definitionen av fri programvara<sup>63</sup> och enligt definitionen av öppen programvara<sup>64</sup>).

Det finns betydande osäkerhet avseende hur FOSS ska uppfattas i olika språkversioner av *CRA*. Detta orsakar en avkylande effekt för internationella affärer. Denna osäkerhet orsakar hinder för internationell samverkan genom FOSS projekt och riskerar orsaka onödiga hinder för global samverkan genom innovativa och affärskritiska FOSS projekt.

Utifrån detta hade det varit önskvärt om *betänkandet* uppmärksammat behovet av vägledning för alla intressenter som i Sverige kan komma påverkas av *CRA*.

---

59 (van der Jeught, 2018, 2025; Schilling, 2020; Taylor, 2011)

60 (Lundell, 2024a, 2024b)

61 (FSD, 2026)

62 (OSD, 2026)

63 (FSD, 2026)

64 (OSD, 2026)

## Sekretess relaterat rapportering av sårbarheter

Många programvaruprojekt utvecklas i en global samverkan och tillhandahållen programvara används i många olika miljöer och jurisdiktioner.

Ett stort antal programvaruprojekt som utvecklar och tillhandahåller FOSS på publikt tillgängliga plattformar involverar ofta ett stort antal individer som, i olika roller, bidrar till utvecklingen utifrån olika incitament. Många FOSS-projekt involverar individer och organisationer från många länder i en global samverkan<sup>65</sup>.

Det är vanligt att enskilda individer som är anställda i, eller engagerade via tidsbegränsade kontrakt av, olika organisationer på olika sätt bidra till den utveckling av FOSS som sker inom ramen för sina respektive engagemang med olika FOSS-projekt<sup>66</sup>. Det är långt ifrån ovanligt att utvecklare som är anställda i företag och andra typer av organisationer på betald arbetstid bidrar till utvecklingen inom FOSS-projekt utifrån den egna organisationens strategiska behov<sup>67</sup>.

Då en sårbarhet upptäcks i en programvara behöver denna sårbarhet, självklart, skyndsamt rapporteras och åtgärdas i enlighet med de krav som ställs av CRA. För sårbarheter som upptäcks inom globalt tillhandahållen FOSS som utvecklats av FOSS projekt som förvalta på publikt tillgängliga publika plattformar (som exempelvis Github och Gitlab) är det vanligt att många individer och organisationer, som är baserade i olika länder, är involverade. Av dessa skäl är det troligt att bestämmelserna i offentlighets- och sekretesslagen<sup>68</sup> (2009:400) i många av dessa fall inte träffar de individer och organisationer som behöver involveras för att kunna åtgärda en sårbarhet. Utifrån detta hade det varit önskvärt att *betänkandet* redovisat en analys av hur offentlighets- och sekretesslagen (2009:400) är tillämplig på de scenarier som blir följden av en situation då uppgifter om sårbarheter behöver kunna delas globalt med de aktörer som har nödvändig kompetens för att kunna åtgärda identifierade brister.

Mot bakgrund av att ENISA idag använder en webbplats som orsakar ett röjande av uppgifter (enligt offentlighets- och sekretesslagen (2009:400)) som en konsekvens av att molntjänster med okända underleverantörer<sup>69</sup> används ställer vi oss frågande till att *betänkandet* inte inkluderar en analys av hur sekretess avseende uppgifter om sårbarheter ska kunna upprätthållas av alla berörda aktörer och intressenter. Vidare har det, för använda molntjänster, identifierats tekniska brister som rapporteras av säkerhetsforskare vid en internationell konferens<sup>70</sup> och som behandlats under seminarium i Sveriges riksdag den 12 november 2025<sup>71</sup> samt under konferensen 'Konkurrens bland molnen' som arrangeras på Högskolan i Skövde den 29 april 2026<sup>72</sup>.

Utifrån detta hade det varit lämpligt att *betänkandet* inkluderat ett förslag om att genomföra en utredning som analyserar huruvida (och i så fall hur) det med tilltänkt process inom CRA kommer att vara möjligt att undvika ett omedelbart röjande av uppgifter om sårbarheter då svenska intressenter ska efterleva CRA. Utan en sådan analys förefaller förslaget om en förändrad offentlighets- och sekretesslagen (2009:400) med nya regler för sekretess helt verkningslösa.

---

65 (Blind et al., 2021)

66 (Butler et al., 2021)

67 (Lundell et al., 2022)

68 (SFS, 2009)

69 (EDPB, 2023a, 2023b)

70 (Hertogh et al., 2026)

71 (Lundell, 2025c, 2025d)

72 (Catry, 2026a, 2026b, 2026c)

## Behov av ytterligare preciseringar och konsekvensbedömningar

Det är en brist att *betänkandet* inte uppmärksammar att den konsekvensbedömning<sup>73</sup> som genomförts inom EU av ett tidigt utkast till *CRA* på avgörande sätt har ett innehåll som avviker från den publicerade förordningen (*CRA*).

Det hade varit lämpligt att *betänkandet* uppmärksammat att det för enskilda intressenter kan vara svårt att avgöra huruvida, samt i så fall på vilka sätt, en enskild intressenten träffas av *CRA*. Utifrån detta hade det varit lämpligt att *betänkandet* föreslagit utveckling av en vägledning som specifikt fokuserar på vilka intressenter och vilka situationer som träffas av *CRA* för speciellt fokus på ett svenskt kontext.

Det är positivt att *betänkandet* föreslår stöd och utveckling av vägledning för mikroföretag och små och medelstora företag, men det hade varit lämpligt att även utvidga detta till andra typer av organisationer. Exempelvis för lärosäten där det är vanligt att enskilda forskare och forskningsprojekt, ofta i samverkan med kommersiella samverkanspartners inom ramen för olika tillämpade forskningsprojekt, etablerar nya (samt bidrar till redan etablerade) programvaruprojekt där utvecklade programvara (ofta) tillhandahålls som FOSS.

Avslutningsvis vill jag tacka för möjligheten att lämna detta yttrande och vill samtidigt tillerkänna utredningen haft ett uppdrag att analysera en mycket komplex uppgift.

Professor Björn Lundell, Ph.D.  
Software Systems Research Group  
Högskolan i Skövde

E-post: [bjorn.lundell@his.se](mailto:bjorn.lundell@his.se)

---

73 (EU, 2022a, 2022b, 2022c, 2022d, 2022e)

## Källhänvisningar

Blind, K., Böhm, M., Grzegorzewska, P., Katz, A., Muto, S., Pätsch, S. & Schubert, T. (2021) The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy, Final Study Report, European Commission, Brussels, ISBN 978-92-76-30980-2.

Brånby, C. & Nilsson, C. (2025) Cyberresiliensförordningen – nya krav för uppkopplade produkter och tjänster, Svenskt näringsliv (Swedish Enterprise), Stockholm, 26 februari.

Butler, S., Gamalielsson, J., Lundell, B., Brax, C. Sjöberg, J., Mattsson, A., Gustavsson, T., Feist, J. & Lönroth, E. (2021) On Company Contributions to Community Open Source Software Projects, IEEE Transactions on Software Engineering, Vol. 47(7), pp. 1381-1401.

Catry, A. (2026a) [https://www.linkedin.com/posts/catry\\_the-chain-of-flawed-reports-occurs-through-activity-7436873030838067200-rxuv](https://www.linkedin.com/posts/catry_the-chain-of-flawed-reports-occurs-through-activity-7436873030838067200-rxuv)

Catry, A. (2026b) [https://www.linkedin.com/posts/catry\\_cybersecurity-datasovereignty-microsoft365-share-7443628081958776832-7rZJ](https://www.linkedin.com/posts/catry_cybersecurity-datasovereignty-microsoft365-share-7443628081958776832-7rZJ)

Catry, A. (2026c) Marknadsföring som efterlevnadsmodell för molntjänster, Inbjuden presentation: Konkurrens bland molnen, 29 april. [https://www.ssr.info/konkurrens-bland-molnen\\_catry/](https://www.ssr.info/konkurrens-bland-molnen_catry/)

Chiara, P. G. (2022) The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements, International Cybersecurity Law Review, Vol. 3, pp. 255-272.

Colonna, L. (2025) The end of open source? Regulating open source under the cyber resilience act and the new product liability directive, Computer Law & Security Review, Vol. 56, 106105.

EDPB (2023a) 2022 Coordinated Enforcement Action: Use of cloud-based services by the public sector, European Data Protection Board, Adopted on 17 January.

EDPB (2023b) Annex: National Reports on the CEF cloud action, European Data Protection Board, Adopted on 17 January.

EU (2022a) Cyber Resilience Act – Impact assessment, European Commission, 15 September.

EU (2022b) Commission Staff Working Document – Impact Assessment Report, *Accompanying the document*: Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 {COM(2022) 454 final} - {SEC(2022) 321 final} - {SWD(2022) 283 final}, SWD(2022) 282 final, Part 1/3, European Commission, 15 September.

EU (2022c) Commission Staff Working Document – Impact Assessment Report, *Accompanying the document*: Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 {COM(2022) 454 final} - {SEC(2022) 321 final} - {SWD(2022) 283 final}, SWD(2022) 282 final, Part 2/3, European Commission, 15 September.

EU (2022d) Commission Staff Working Document – Impact Assessment Report, *Accompanying the document*: Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 {COM(2022) 454 final} - {SEC(2022) 321 final} - {SWD(2022) 283 final}, SWD(2022) 282 final, Part 3/3, European Commission, 15 September.

EU (2022e) Commission Staff Working Document – Executive Summary of the Impact Assessment Report, *Accompanying the document*: Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 {COM(2022) 454 final} - {SEC(2022) 321 final} - {SWD(2022) 283 final}, SWD(2022) 283 final, European Commission, 15 September.

EU (2022f) European Commission, Commission Notice: The ‘Blue Guide’ on the implementation of EU product rules 2022, C 247/1, Official Journal of the European Union, 29 June.

EU (2022g) Europeiska Kommissionen, Meddelande från kommissionen, 2022 års blåbok om genomförandet av EU:s produktbestämmelser, C 247/1, Europeiska unionens officiella tidning, 29 juni.

EU (2024a) Cyber Resilience Act: European Parliament legislative resolution of 12 March 2024 on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)), European Parliament, 12 March.

EU (2024b) Förordning om cybersäkerhet: Europaparlamentets lagstiftningsresolution av den 12 mars 2024 om förslaget till Europaparlamentets och rådets förordning om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)), Europaparlamentet, 12 mars.

EU (2024c) Corrigendum to the position of the European Parliament adopted at first reading on 12 March 2024 with a view to the adoption of Regulation (EU) 2024/ ... of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (COM(2022)0454 ; C9-0308/2022 ; 2022/0272(COD)), European Parliament, 18 July.

EU (2024d) Rättelse till Europaparlamentets ståndpunkt fastställd vid första behandlingen den 12 mars 2024 inför antagandet av Europaparlamentets och rådets förordning (EU) 2024/... om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensakten) (COM(2022)0454 ; C9-0308/2022 ; 2022/0272(COD)), Europaparlament, 23 juli.

EU (2024e) Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 - Outcome of the European Parliament's first reading and Corrigendum procedure (Strasbourg, 12 March 2024 and Strasbourg, 17 September 2024), Council of the European Union, 23 September.

EU (2024f) Förslag till Europaparlamentets och rådets förordning om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020 – Resultatet av Europaparlamentets första behandling samt rättelseförfarande (Strasbourg den 12 mars 2024 och Strasbourg den 17 september 2024), Europeiska unionens råd, 23 september.

EU (2024g) Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), The European Parliament and the Council of the European Union, 25 September.

EU (2024h) Europaparlamentets och rådets förordning om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen), Europaparlamentet och Europeiska unionens råd, 25 september.

EU (2024i) Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirement for Products with Digital Elements and Amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), PE 100 2023 REV 1, The European Parliament and the Council of the European Union, 23 October.

EU (2024j) Europaparlamentets och rådets förordning om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) Nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (Cyberresiliensförordningen), Europaparlamentet och Europeiska unionens råd, 23 oktober.

EU (2024k) Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), Official Journal of the European Union, 20 November.

EU (2024l) Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen), Europeiska unionens officiella tidning, 20 november.

EU (2025a) Commission Implementing Decision of 3.2.2025 on a standardisation request to the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), C(2025) 618 final, European Commission, 3 February.

EU (2025b) Annexes to the Commission Implementing Decision on a standardisation request to the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), C(2025) 618 final Annexes 1 to 2, European Commission, 3 February.

EU (2025c) Commission Implementing Regulation (EU) 2025/2392 of 28 November 2025 on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council, Official Journal of the European Union, 1 December.

EU (2025d) Kommissionens genomförandeförordning (EU) 2025/2392 av den 28 november 2025 om den tekniska beskrivningen av kategorierna av viktiga och kritiska produkter med digitala element enligt Europaparlamentets och rådets förordning (EU) 2024/2847, Europeiska Unionens Officiella tidning, 1 december.

EU (2025e) Cyber Resilience Act, European Commission, 3 December.

EU (2025f) The Cyber Resilience Act – Summary of the legislative text, European Commission, 3 December.

EU (2026) FAQs on the Cyber Resilience Act, European Commission, Version 1.2, 16 January.

FSD (2026) The Free Software Definition, The Free Software Foundation.  
<https://www.gnu.org/philosophy/free-sw.en.html#fs-definition> (As is: 7 April 2026).

FSF (2026) The Free Software Foundation. <https://www.fsf.org/> (As is: 7 April 2026).

Georgiadou, I., Gavrila, R., Łokietek, T., Sroka, K. & Czyż, A. (2025) SBOM Landscape Analysis: Towards an Implementation Guide, European Union Agency for Cybersecurity, ENISA, Draft 1.2, December. [https://www.enisa.europa.eu/sites/default/files/2025-12/SBOM%20Analysis%20-%20Towards%20an%20Implementation%20Guide\\_v1.20-Published.pdf](https://www.enisa.europa.eu/sites/default/files/2025-12/SBOM%20Analysis%20-%20Towards%20an%20Implementation%20Guide_v1.20-Published.pdf)

González-Barahona, J. M. (2004) Quo vadis, libre software?, v0.8.1, September.  
<https://web.archive.org/web/20041207003919/http://sinetgy.org/jgb/articulos/libre-software-origin/>

Gonzalez-Barahona, J. (2021) A Brief History of Free, Open Source Software and Its Communities, Computer, Vol. 54(2), pp. 75-79.

Hertogh, M., Quakkelaar, D., Raymakers, T., Sarma, M. H., Muench, M., Bos, H. & van der Kouwe, E. (2026) Rain: Transiently Leaking Data from Public Clouds Using Old Vulnerabilities, In 2026 IEEE Symposium on Security and Privacy (SP), IEEE Computer Society, Los Alamitos, pp. 1189-1205.

van der Jeught, S. (2018) Current Practices with regard to the Interpretation of Multilingual EU Law: How to Deal with Diverging Language Versions?, European Journal of Legal Studies, Vol. 11(1), pp. 5-38.

van der Jeught, S. (2025) The Multilingualism Paradox in EU Law: In Our Own Language Version We Trust, *International Journal of Language & Law (JLL)*, Vol. 14, pp. 81-98.

Johnson, L. (1998) A view from the 1960s: how the software industry began, *IEEE Annals of the History of Computing*, Vol. 20(1), pp. 36-42.

Kamara, I. (2024). European cybersecurity standardisation: a tale of two solitudes in view of Europe's cyber resilience, *Innovation: The European Journal of Social Science Research*, Vol. 37(5), pp. 1441-1460.

Kikelj, M. & Sabic, I. (2024) Strengthening the Digital Ecosystem: Effects of the Cyber Resilience Act (CRA) on Open-Source Software, In 2024 IEEE International Conference on Cyber Security and Resilience (CSR), London, pp. 557-561.

Lasota, L. (2025) The CRA and the Challenges of Regulating Cybersecurity in Open Environments: The Case of Free and Open Source Software, In Gsenger, R. & Sekwenz, M.-T. (Eds.), *Digital Decade: How the EU Shapes Digitalisation Research*, Nomos, Baden-Baden, pp. 445-477.

Lundell, B. (2020) Analys av DIGG:s policy för utveckling av programvara, Högskolan i Skövde, Skövde, ISBN: 978-91-983667-6-1, 100p, <http://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-18895>

Lundell, B. (2021) Yttrande över betänkandet Säker och kostnadseffektiv IT-drift (SOU 2021:1), Dnr. HS 2021/469, Högskolan i Skövde, Skövde, 7 maj (*Yttrandet skickat till Finansdepartementet, Stockholm*).

Lundell, B. (2022a) Enskilt yttrande över Riksarkivets förslag till författningar (Dnr. RA-KS 2021/18), Dnr. HS 2021/842, Högskolan i Skövde, Skövde, 28 januari (*Yttrandet skickat till Riksarkivet, Stockholm*).

Lundell, B. (2022b) Yttrande över betänkandet Säker och kostnadseffektiv IT-drift (SOU 2021:97), Version 1.0, Dnr. HS 2022/245, Högskolan i Skövde, Skövde, 21 mars (*Yttrandet skickat till Finansdepartementet, Stockholm*).

Lundell, B. (2022c) Feedback to the European Commission's Call for Evidence for an impact assessment on Intellectual Property – new framework for standard essential patents (SEPs), 9 May, published as feedback reference: F3257432, European Commission.

Lundell, B. (2023a) Comments on the European Commission proposal for a Regulation on SEPs, Dnr. HS 2023/568, Högskolan i Skövde, Skövde, 10 August, also published as feedback reference: F3434461, European Commission.

Lundell, B. (2023b) Yttrande över lagförslag till EU:s Cyber Resilience Act, Version 1.0, Dnr. HS 2023/495, Högskolan i Skövde, Skövde, 19 juni (*Yttrandet skickat till Carl-Oskar Bohlin, Minister för civilt försvar, Försvarsdepartementet & Regeringskansliet*).

Lundell, B. (2023c) Yttrande över lagförslag till EU:s Cyber Resilience Act, Version 2.1, Dnr. HS 2023/495, Högskolan i Skövde, Skövde, 28 augusti (*Yttrandet skickat till Erik Slottnér, Civilminister, Finansdepartementet & Regeringskansliet*).

Lundell, B. (2024a) Openness Concepts and Translation Incoherence: Clarifying the EU Cyber Resilience Act (CRA), Version 1.0 (Dnr. FP 2024/30), Högskolan i Skövde, 25 April (*Yttrandet skickat till Benjamin Bögel, Policy Officer on Cyber Security, European Commission*).

Lundell, B. (2024b) Openness Concepts and Inconsistencies between different language versions of the EU Cyber Resilience Act (CRA), Version 2.0 (Dnr. FP 2024/30), Högskolan i Skövde, 8 October (*Yttrandet skickat till Benjamin Bögel, Policy Officer on Cyber Security, European Commission*).

Lundell, B. (2025a) Yttrande över betänkandet AI-kommissionens Färdplan för Sverige (SOU 2025:12), Version 1.0, Dnr. HS 2025/373, Högskolan i Skövde, Skövde, 3 juni (*Yttrandet skickat till Finansdepartementet, Stockholm*).

Lundell, B. (2025b) Comments on the Revision of the Standardisation Regulation, Dnr. HS 2025/450, Högskolan i Skövde, Skövde, 21 July, also published as feedback reference: F3581814, European Commission.

Lundell, B. (2025c) Användning av molntjänster under okända villkor inom riksdagen – konsekvenser av att använda Microsoft 365 och Microsoft Teams (M365): Varför anskaffar myndigheter Microsoft 365 – genom en bakvänd anskaffningsprocess utan föregående konkurrensutsättning (där myndigheter underlåter att anskaffa alla nödvändiga licenser) – för att behandla känsliga uppgifter under okända villkor (och genom denna behandling orsaka ett olämpligt röjande av känsliga uppgifter)?, Presentation under seminarium om tilltänkt användning av Microsoft 365 och Microsoft Teams inom riksdagen, Sveriges riksdag, 12 november.

Lundell, B. (2025d) Seminarium om tilltänkt användning av Microsoft 365 inom riksdagen: Observationer från analys av förstudierrapporten och obesvarade frågor, Rapport till Riksdagsförvaltningen (med frågor från seminarium i riksdagen), Sveriges riksdag, 17 November.

Lundell, B. (2026a) Contributions to the ‘Open Consultation on the SBOM Implementation Guide’, SBOM Landscape Analysis - Towards an Implementation Guide, European Union Agency for Cybersecurity (ENISA), 16 January.

Lundell, B. (2026b) Comments on the revision of EU rules on public procurement, Dnr. HS 2026/81, Högskolan i Skövde, Skövde, 25 January, Feedback concerning ‘Revision of EU rules on public procurement’, also published as feedback reference: F33367416, European Commission.

Lundell, B., Butler, S., Fischer, T., Gamalielsson, J., Brax, C., Feist, J., Gustavsson, T., Katz, A., Kvarnström, B., Lönroth, E. & Mattsson, A. (2022) Effective Strategies for Using Open Source Software and Open Standards in Organizational Contexts – Experiences From the Primary and Secondary Software Sectors, IEEE Software, Vol. 39(1), pp. 84-92.

Lundell, B., Gamalielsson, J. & Tengblad, S. (2016) IT-standarder, inlåsning och konkurrens: En analys av policy och praktik inom svensk förvaltning, Uppdragsforskningsrapport 2016:2, Konkurrensverket, ISSN: 1652-8089.

Lundell, B., Lings, B. & Lindqvist, E. (2006) Perceptions and Uptake of Open Source in Swedish Organisations, In Damiani et al. (Eds.) Open Source Systems: IFIP Working Group 2.13 Foundation Conference on Open Source Software – The Second International Conference on Open Source Systems, Vol. 203, Springer, Boston, pp. 151-163.

NPS (2016) Open IT-standards, National Procurement Services (Kammarkollegiet), Stockholm, Dnr 96-38-2014, 7 March. <https://www.avropa.se/globalassets/dokument/open-it-standards.pdf>

OSD (2026) The Open Source Definition, Version 1.9, Open Source Initiative, Last modified 22 March 2007. <https://opensource.org/osd> (As is: 7 April 2026).

OSI (2026) Open Source Initiative. <https://opensource.org/> (As is: 7 April 2026).

Riehle, D. (2009) The Commercial Open Source Business Model, In Nelson, M. L. (Eds.) Value Creation in e-Business Management, Springer-Verlag, Berlin, pp. 18-30.

Schilling, T. (2020) Beyond Multilingualism: On Different Approaches to the Handling of Diverging Language Versions of a Community Law, European Law Journal, Vol. 16(1), pp. 47-66.

State Chancellery (2024) Open Innovation and Open Source Strategy of Land Schleswig-Holstein, The Minister-President, State Chancellery, Kiel, Version 1.00, 20 November.

SFS (2009) Offentlighets- och sekretesslag (2009:400), SFS nr: 2009:400, 20 maj.

SOU (2025) Kompletterande bestämmelser till EU:s cyberresiliensförordning, Statens Offentliga Utredningar, SOU 2025:115, Betänkande av Cyberresiliensutredningen, Stockholm, ISBN ISBN 978-91-525-1422-1.

Taylor, S. (2011) The European Union and National Legal Languages: An Awkward Partnership? Revue française de linguistique appliquée, Vol. XVI(1), 105-118.

Teichmann, F. (2026) The cyber resilience act as a new paradigm for product security: a compliance roadmap, International Cybersecurity Law Review, Vol. 7, pp. 1-17.

Teichmann, F. & Sergi, B. S. (2025) The EU Cyber Resilience Act: Hybrid governance, compliance, and cybersecurity regulation in the digital ecosystem, Computer Law & Security Review, Vol. 59, 106209.

Tridgell, J. & Singh, J. (2025) 'Stewardship' as a Fair, Accountable and Transparent Model for Free and Open-Source Software Governance? Looking Beyond the EU's Cyber Resilience Act, In Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency, ACM, New York, pp. 473-484.