

New Challenges for the Medical Devices' Cybersecurity in the EU

Elisabetta Biasin,
Erik Kamenjasevic

KU Leuven Centre for IT & IP Law (CiTiP) – imec

2nd ECSCI Online Workshop on Critical Infrastructure Protection
Wednesday, 27 April 2022

Based on: Biasin & Kamenjasevic (forthcoming) Cybersecurity of Medical Devices: New Challenges Arising from the AI Act and NIS 2 Directive Proposals

Content

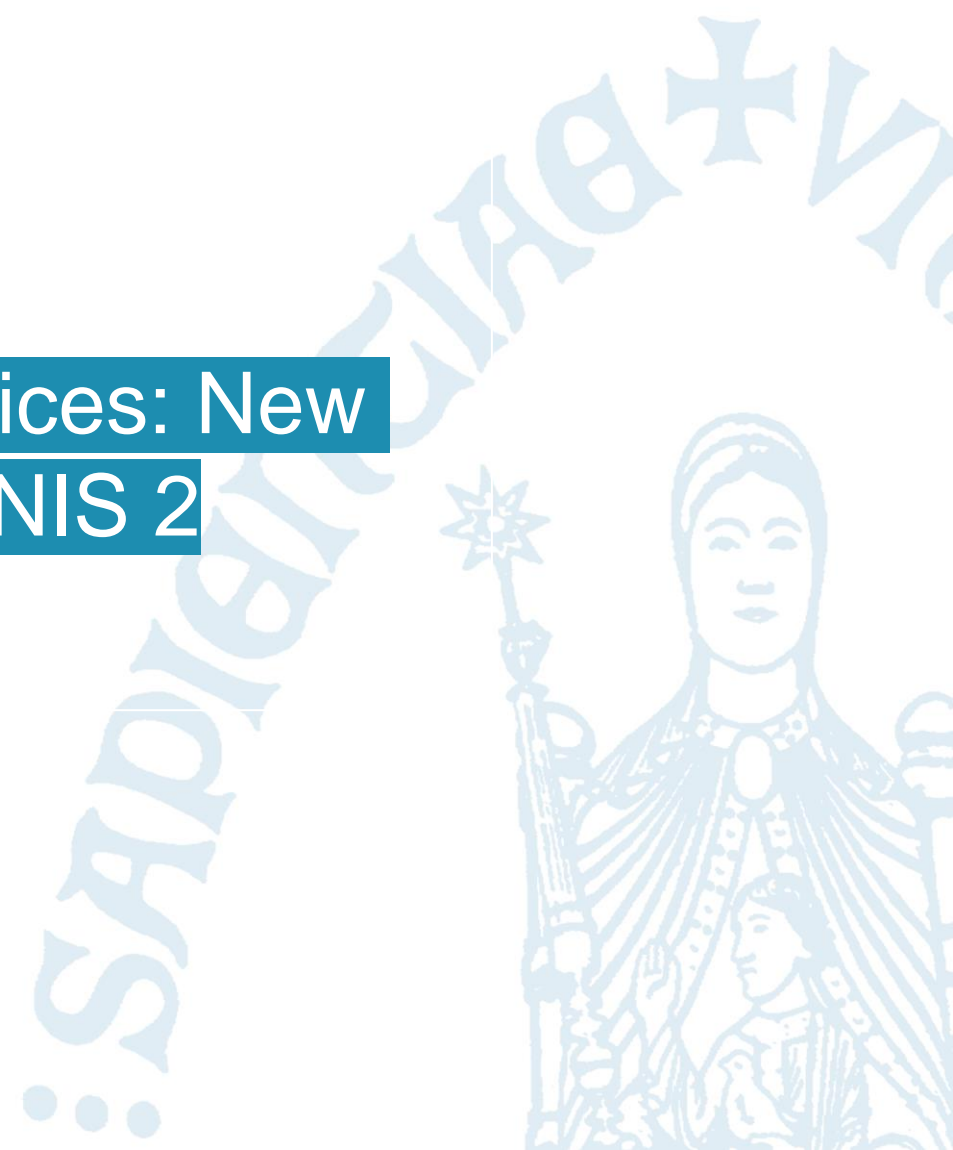
1) Cybersecurity of Medical Devices

2) Paper: Cybersecurity of Medical Devices: New Challenges Arising from the AI Act and NIS 2

Directive Proposals

3) The four core challenges

4) Recommendations



Cybersecurity of Medical Devices



Playing with Lives: Cyberattacks on Healthcare are Attacks on People

March 2021

Executive Summary

Online or offline, attacking healthcare is attacking people. As a critical and

the people it serves. Our objectives are to de-escalate the number and magnitude of

GUIDANCE DOCUMENT

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Draft Guidance for Industry and Food and Drug Administration Staff

APRIL 2022

[Download the Draft Guidance Document](#)

[Read the Federal Register Notice](#)

Draft

Not for implementation. Contains non-binding recommendations.

This guidance is being distributed for comment purposes only.

AI

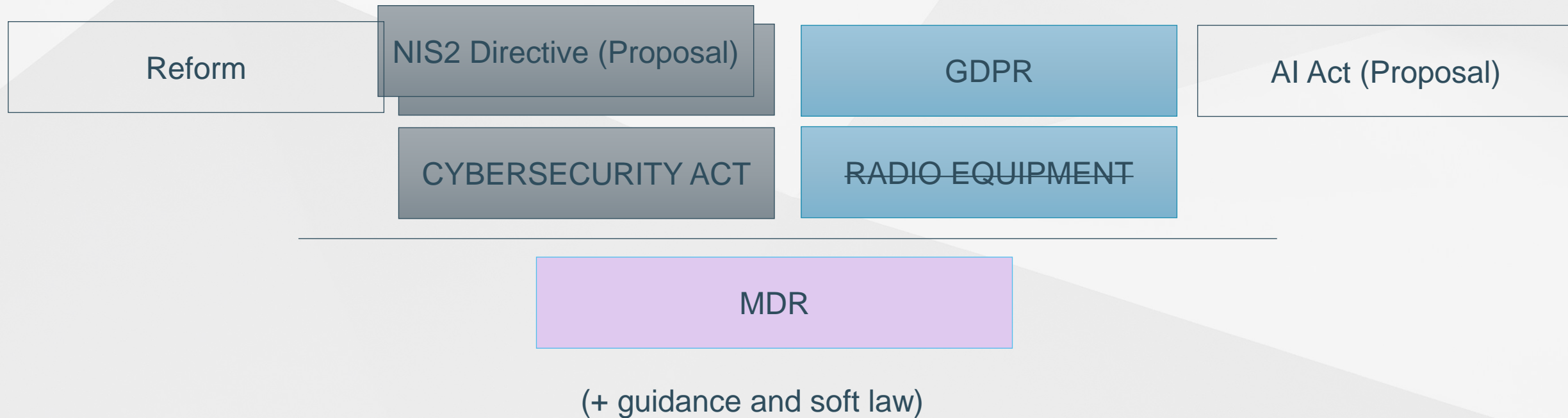
**Software as a Medical Device
Medical Device Software**



Paper: Cybersecurity of Medical Devices: New Challenges Arising from the AI Act and NIS 2 Directive Proposals



MD Cybersecurity – Relevant EU Laws



Shapenlined on Unsplash

EU Law Analysis: MDR &



“NIS 2.0” Proposal



AI Act Proposal

Christian Lue on Unsplash

Core challenges

Focus: Regulatory convergence on incident notification requirements



The NIS 2 Directive Proposal

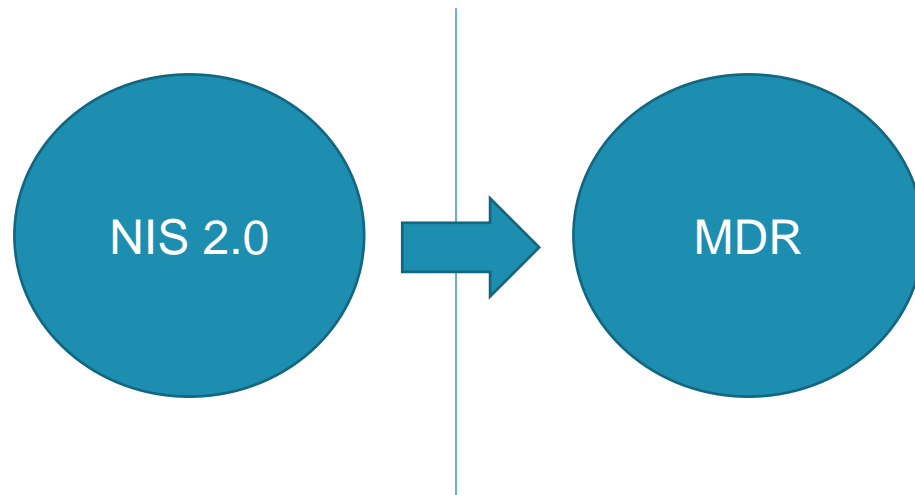
Incident notification

1) Incident notification

(NIS 2.0 and the MDR)

MDR = Lex Specialis

IF notification obligations “at least equivalent”



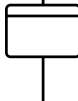




The notion of “at least equivalent” is UNCLEAR

1) Incident notification

(NIS 2.0 and the MDR)

Analysis: Divergences between the acts

Regulated entities		<i>CE EE/Manufacturers</i>
Definition		<i>Incident/Serious incident (*cyber threat)</i>
Event		<i>Potential or occurred</i>
Timing		<i>24h/15d</i>
Authorities		<i>CSIRT CA/ CA</i>

1) Incident notification

(NIS 2.0 and the MDR)

Focus: Definition – Security incident do not always equate to safety incident



Example: Warming therapy device for premature babies (from MDCG, 2019)

1) Incident notification

(NIS 2.0 and the MDR)



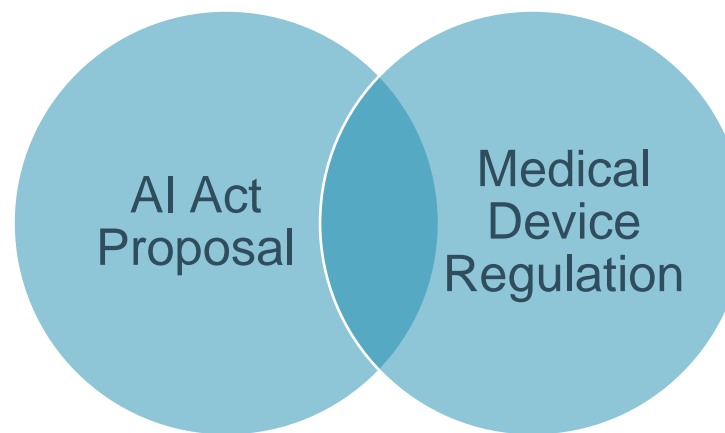
The AI Act proposal

Serious incident

2) Cybersecurity requirements

(AI Act and the MDR)

AI Act Serious incident ≠ MDR Serious incident



***AI Act proposal might have broader application,
UNSPECIFIED Interaction with MDR***

2) Cybersecurity requirements

(AI Act and the MDR)

Example of cybersecurity incident that may be an AI incident



Anesthesia device (from MDCG 2019)

Terminological Consistency

3) “Cybersecurity”

Inconsistent use

4) “Critical Infrastructures”

Risks of fragmentation in the EU
market



Recommendations





1

NIS 2.0/MDR: Incident notification: ‘**at least equivalent**’ – indicate what applies (3 options)

2

AI Act/MDR: **cybersecurity requirements**: expand explanatory remarks on their interplay, and address convergence issues



3

NIS2: ‘Cybersecurity’ more coherent use in the proposal – **‘NIS’** for technical contexts (cf EDPS, 2021)

4

AI Act: ‘Critical infrastructures’: limit to the extent possible, the diverging interpretation at the national level. Provide further clarifications or references to the healthcare sector for serious incidents

Thank you!

Cybersecurity of medical devices: Regulatory challenges in the EU

In I. Cohen, T. Minssen, W. Price II, C. Robertson, & C. Shachar (Eds.), *The Future of Medical Device Regulation: Innovation and Protection* (pp. 51-62). Cambridge: Cambridge University Press.
doi:10.1017/9781108975452.005



Cybersecurity of Medical Devices: New Challenges Arising from the AI Act and NIS 2 Directive Proposals

*

TUFTS Student Symposium in Cybersecurity Policy/ EAHL



Funding acknowledgement

SAFEACRE has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 787002

KU Leuven Centre for IT & IP Law (CiTiP) - imec
Sint-Michielsstraat 6, box 3443
BE-3000 Leuven, Belgium

<http://www.law.kuleuven.be/citip>

These slides are released under the following Creative Commons
License: Attribution - 4.0 International (CC BY)