The Internet of Things and Cybersecurity from a Legal Perspective

25-10-2023 – ACCSS PhD Lunch
Mattis van ‘t Schip
Ph.D. Candidate – Radboud University (iHub)

Radboud University

THE INTERNET OF THINGS: STRUGGLES IN THE INDUSTRY

- The Internet of Things industry
  - Rapid development of new products/series
  - Quick product-to-market action
  - Spreading processing power across various devices

- Leading to…
  - Cybersecurity problems (“The S in IoT stands for security”)
  - Data protection issues (e.g., remote access to IP cameras)

- Unfortunately…
  - A legal gap to address these issues

PERSISTENT LEGAL GAP

- "The EU is conducting a DDoS attack on legal scholars!"
- Recent legislation concerning digitalisation:
  - Cybersecurity Act (procedural, set-up of ENISA)
  - Cyber Resilience Act (cybersecurity rules for software and hardware products)
  - New Product Liability Directive (when software causes physical damages)
  - NIS2 Directive (for critical and important entities in e.g., the health and energy sector)
  - Digital Operational Resilience Act (financial entities)
  - General Data Protection Regulation
  - AI Act
  - Radio Equipment Directive
  - Digital Markets Act
  - Digital Services Act
  - ePrivacy Directive
  - Cyber Solidarity Act (forthcoming)
  - …

PERSISENT LEGAL GAP

- “The EU is conducting a DDoS attack on legal scholars”
- Recent legislation concerning digitalisation:
  - Cybersecurity Act (procedural, set-up of ENISA)
  - **Cyber Resilience Act** (cybersecurity rules for software and hardware products)
  - **New Product Liability Directive** (when software causes physical damages)
  - **NIS2 Directive** (for critical and important entities in e.g., the health and energy sector)
  - Digital Operational Resilience Act (financial entities)
  - **General Data Protection Regulation**
  - AI Act
  - Radio Equipment Directive
  - Digital Markets Act
  - Digital Services Act
  - ePrivacy Directive
  - Cyber Solidarity Act (forthcoming)
  - …

WHO IS RESPONSIBLE?

- An Internet of Things device is created by:
  - Software developers (cloud providers, operating system developers, etc.)
  - Hardware manufacturers (watch components, battery components, etc.)
- Meanwhile, our existing legal frameworks address:
  - Data processing (General Data Protection Regulation)
  - Manufacturers, importers, and distributors (Radio Equipment Directive/Cyber Resilience Act)
- What about…
  - The *entire* supply chain (manufacturer to seller and user)
  - Open-source developers (Log4j)
  - And other involved actors?

A SNEAK PEEK OF CURRENT WORK: NIS2 DIRECTIVE & SUPPLY CHAIN SECURITY

- What about…
  - The *entire* supply chain

- The NIS2 Directive mandates “supply chain security measures” for entities in critical sectors
  - Hospitals, energy companies, manufacturing industry, space industry, etc.
  - What is the supply chain?
  - What is supply chain security? What measures are included?
  - NIS2 Directive is unclear, while supply chain security is a requirement!

A SNEAK PEEK OF CURRENT WORK: CYBER RESILIENCE ACT & OPEN-SOURCE SOFTWARE

- What about…
  - Open-source developers

- The Cyber Resilience Act (proposal) applies to open-source software development!
  - Only when conducted in the course of a “commercial activity”
  - What is a commercial activity?

  Asking for donations? Requesting a fee? Offering technical support?
  - Unfair responsibilities for open-source software development

A SNEAK PEEK OF CURRENT WORK: CYBER RESILIENCE ACT & OPEN-SOURCE SOFTWARE

- What about…
  - Companies that cease to exist?

- Work-in-progress
- Bankrupt companies no longer have responsibilities
- But what about their cloud servers? Can you just leave consumers with defunct IoT devices?
- Does the “connectedness” of IoT require a new legal framework in such cases?

Thank you!

✉ mattis.vantschip@ru.nl

mattis@eupolicy.social

Radboud University

iHub

This research is funded by the NWO INTERSCT project