The Cyber Resilience Act is finally adopted by Gaelle Le Gars

As a result of my and Rob's earlier participation in the DOSS project, I had the opportunity to pay attention to the increasingly critical issue of 'cybersecurity market surveillance', regarding electronic components imported from outside the EU and, more broadly, to the cybersecurity of those supply chains.

One goal of the DOSS project is the development of a *comprehensive security descriptor* for IoT devices – the "Device Security Passport" – which will find an obvious application now that the Cyber Resilience Act (CRA) is finally adopted. On Friday 11th of October, the text received final approval by the Council of the substantially strengthened version adopted by the European Parliament.

The broader context is the long-standing EU agenda to *digitalise* [every part of] the EU economy. The latest iteration of this agenda, the 'Digital Decade' covers the current decade until 2030 and has already produced multiple laws across different policy domains. The full impact will only be felt over the next 3-5 years when most of them will have come into effect. Put together, these new laws are preparing the ground for a heavily digitalised post-2030 form of governance for the EU. The expected outcome is a set of 'always-on' digital services, built on a dense layer of interoperable systems, data, automated processes and ***digital infrastructures***.

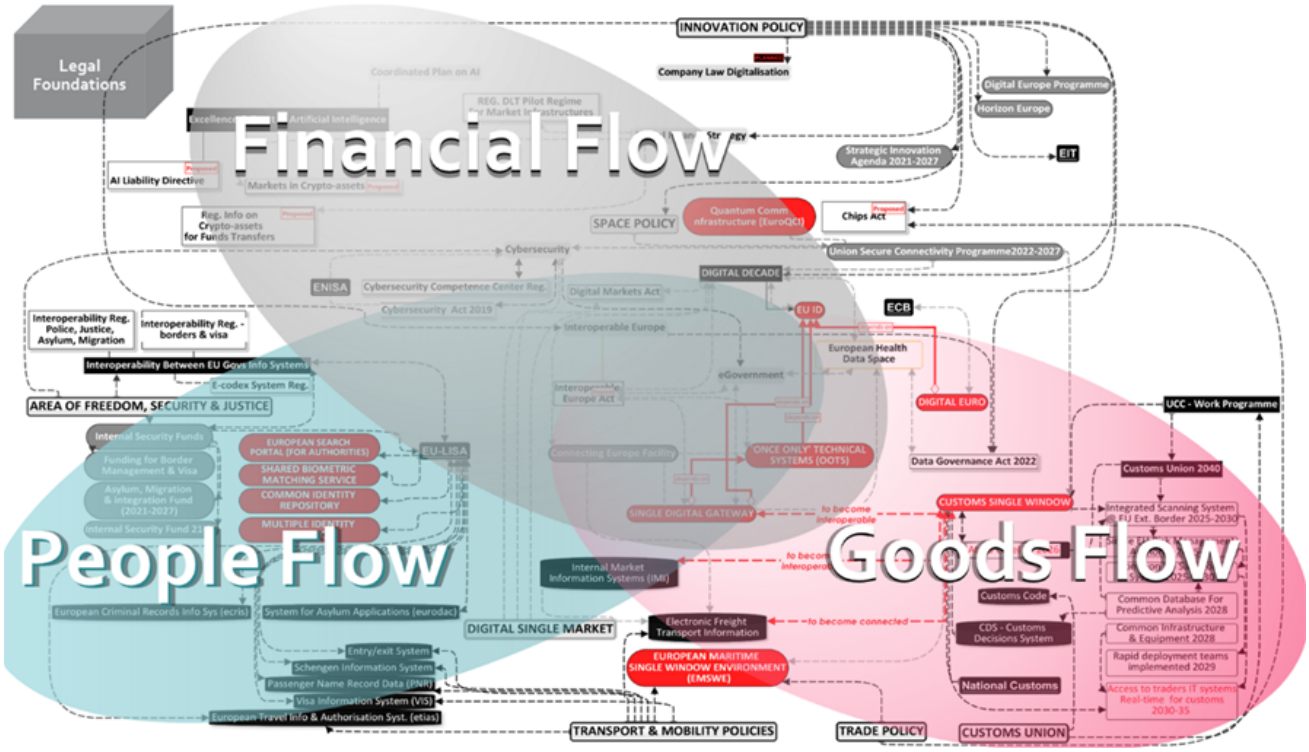
Greater digitalisation comes with greater exposure to cybercrime. Over the same period, a number of laws have been adopted to complete the framework addressing cybersecurity including the cybersecurity act (2019), the NIS2 directive (2022) and most recently the Cyber Resilience Act.

Visualising *Digitalisation* across EU Policies

Back in 2022, looking for a better way to understand the full picture, I set out to produce a visual mapping of the digitalisation component of EU policy agendas by policy area.

The full result is visible here.

What this mapping revealed from the bigger picture, spanning all EU policy domains, could be summarised as the ***digitalisation of three broad flows: people, money and goods.***



What “Digitalising” the flow of goods actually means

The free circulation of goods is one of the three pillars of the EU Single Market. The principle is a single set of rules, uniformly applied across the EU, (& EEA*) to products being placed and remaining available on the market.

The criteria applicable are set by product-specific legislation defining the list of ‘*essential requirements*’ the products covered must meet to obtain approval. Originally called ‘essential safety requirements’, the lists of criteria applicable have expanded to include those set in horizontal legislation (e.g. environment or energy performance). *‘Market Surveillance’* is the set of processes and bodies involved in ensuring that products fulfill those essential requirements applicable to them, before and while on the market. Digitalisation of these important but bureaucratic steps and functions is not new. But the information is gathered across separate systems, siloed by purpose, product category and/or geography.

For the current phase, the drive to further “digitalise” these processes is more about enabling the timely access to relevant data across those different systems by relevant authorities by removing both legal and technical barriers. It also aims to further simplify procedures required of producers through the systematic application of the once-only principle. The need for this arose from the growing volume of non-food goods purchased on digital platform which unlawfully bypass the established “market surveillance” scrutiny and compliance verification steps. The end goal is a digital tracking system documenting compliance, closely following the individual product itself, from conception to decommissioning.

Why the Cyber Resilience Act matters

IoT- and other connected products and related software are prime candidates for this regulatory tracking throughout their life cycle. It is difficult to imagine a better suited industry to implement a ‘digital tracking’ approach to *market surveillance* than the very industry producing the core part of any digital tracking system. Furthermore, as a recent event dramatically illustrated, risks induced by malicious remote access and supply chains tampering persist well beyond the point of purchase with potentially lethal consequences.

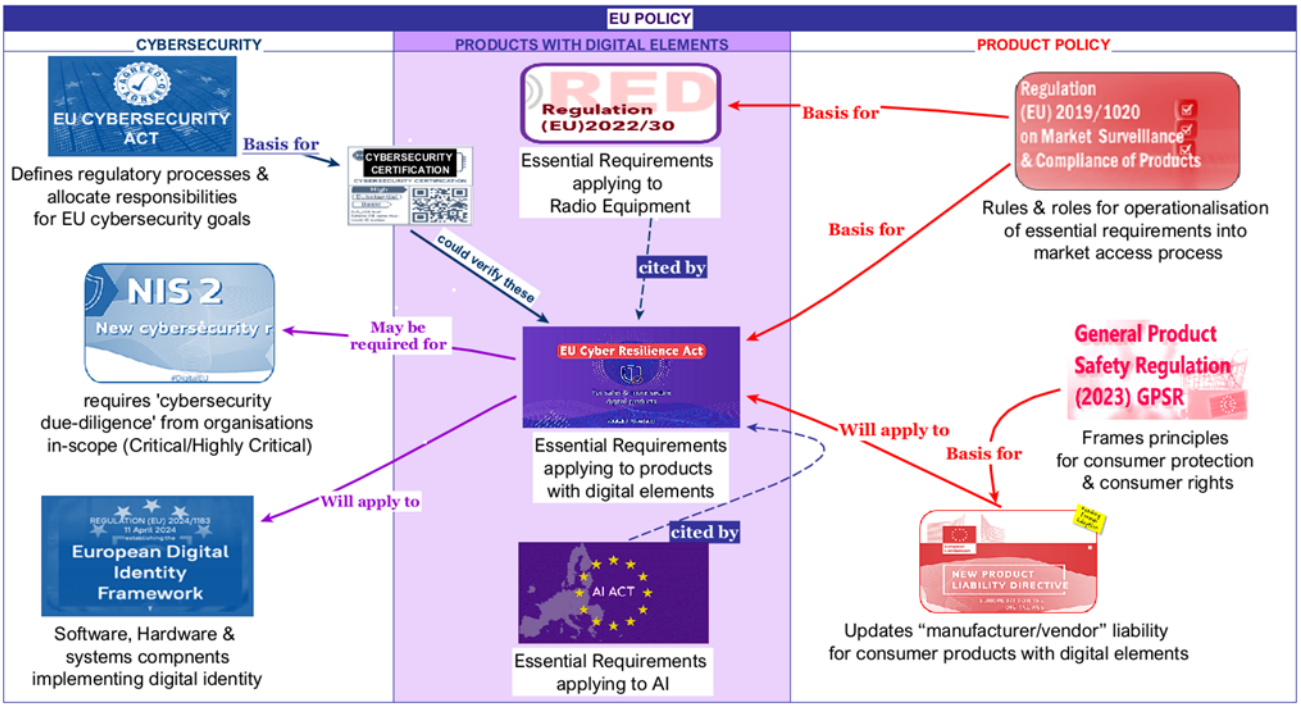
In recent years, cybersecurity-relevant requirements have been added to the list applying to specific products where the cybersecurity risk had a direct relationship to safety risks (e;g; certain medical

devices). But until now, there was no comprehensive set of 'essential requirements' tackling cybersecurity sufficiently broadly to apply to the growing range of connected products and applications and encompassing the full product/component life-cycle.

The Cybersecurity Act (2019) has empowered ENISA to support the development of cybersecurity certification. But those certification schemes are voluntary and driven by changing expectations of the demand-side – which is one intended effect of NIS2. Under NIS2 – coming into effect on 18th October 2024 - a system owner/operator failing to conduct cybersecurity due-diligence on IoT components presenting a risk to its operations, could face substantial administrative fines.

This is where the Cyber Resilience Act will make a real difference.

Although its focus is on cybersecurity, the Cyber Resilience Act is also an integral part of 'market surveillance' legislation. It establishes the cybersecurity *'essential requirements'* applying to products with digital elements.



The final text is lengthy and more comprehensive than would typically be the case for 'market surveillance' legislation. It explicitely considers indirect and second level effect of decisions it empowers authorities to make. It also makes explicit references to "public security" as a legitimate reason to act in specific instances.

The scope is inevitably broad and includes components (see definitions section of the text). It categorises product by risk-level, a common feature of market surveillance laws.

It foresees a number of implementing and enabling acts as well as potential new standards to become fully implementable. Its full effect, including large potential fines for failing to comply, will only be felt from 2028 onwards. The adoption of the CRA could trigger interesting cascading effects on EU customs reform. But this is for a later episode.

Anyone with an eye for the practical implications should start reading it from the annexes where the product scopes and requirements are clearly laid out. Until its official publication, the most recent text is available here.

PE-100-2023-INIT_en.pdf

Gaelle Le Gars. Contact her at gaellelegars at theinternetofthings.eu