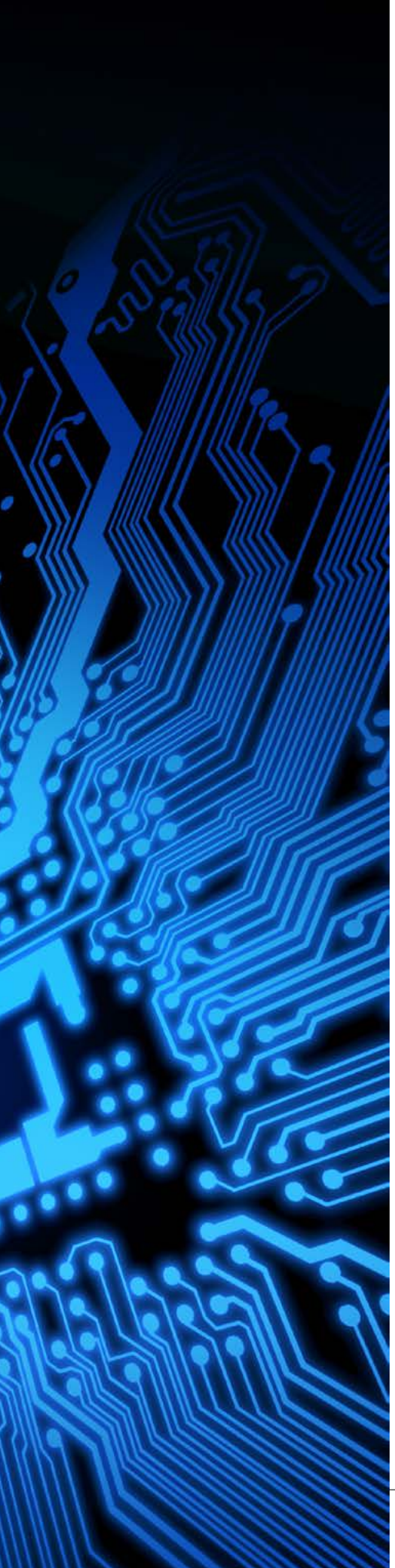
Firewalls and antivirus software have become the Maginot Line of the digital age – static, brittle and ill-suited bulwarks against sophisticated threats.



Europe's invisible battleground: safeguarding the commons in an era of borderless threats

by Aiko Yeo

When ransomware crippled Ireland's national health service in 2021, the nation's lifelines buckled. Monitors went dark, ambulances were diverted, and vital medical records vanished behind encrypted walls. A subsequent government inquiry delivered a brutal verdict: firewalls and antivirus software have become the Maginot Line of the digital age – static, brittle and ill-suited bulwarks against sophisticated threats.

In Western Europe, such episodes are no longer outliers. They are a lived reality. The 2025 Iberian Peninsula blackout illustrates this point: a single breach can cascade across borders and morph into a continental crisis. Herein lies a paradox: digital systems, conceived as the backbone of rights and public utility, can just as quickly become a conduit for their erosion.

When a corrupted electoral register denies citizens the vote or a hacked asylum database strands refugees in legal limbo, the damage is not merely operational. These seismic shocks strike at the core of the region's total defence, where sovereignty, commerce and human rights are woven into the same fabric to secure society.

Against this backdrop, both Brussels and London have advanced flagship regulatory regimes aimed at fortifying Europe's digital ecosystem and softening the blow of the next disruption. This article first charts the protections within each framework and finds that

distinct legal dialects are shaped by policy priorities. Yet, despite divergent legal trajectories, a closer investigation reveals a shared two-pronged ambition. First, to make systemic cyber resilience a default design principle, rooted in resilience engineering and critical infrastructure protection theory. Second, to assign the heaviest duties to the most consequential actors, guided by proportionality, tempered by the precautionary principle, and anchored in a robust framework of duty of care.

Drawing the digital perimeter

Every credible cybersecurity framework first asks a deceptively simple question: Who and what merits protection? The answer reveals far more than technical scope; it exposes a government's priorities and its chosen balance between economic freedom, state oversight and individual rights.

In Brussels, that answer is unapologetically broad. *The Network and Information Security Directive (NIS2) Directive*[1] sweeps "essential" and "important" entities across 18 sectors into its orbit — not just power grids and telecoms, but public administrations, hospitals, managed service providers, and data centres. It signals a deliberate policy shift: resilience is framed not as a perk for critical industries but as a public good embedded in Europe's rights architecture. By incorporating these entities into the sphere of regional cyber defence, Brussels affirms that uninterrupted access is as much about equality as it is about economic necessity. A breach anywhere in any of these nodes then demands the same urgency typically reserved for a public health emergency, or a food safety crises.

Herein lies a paradox: digital systems, conceived as the backbone of rights and public utility, can just as quickly become a conduit for their erosion

The accompanying *Cyber Resilience Act*[2] pushes the perimeter outwards by setting horizontal security standards for any product with "digital elements". Its strategy is to confront systemic risk at the source, shifting accountability upstream to those best positioned to mitigate it, namely manufacturers and suppliers. Supplier-risk management is recast from a peripheral corporate afterthought into a binding legal mandate, harmonising industry practice with the EU's normative commitment to public protection.

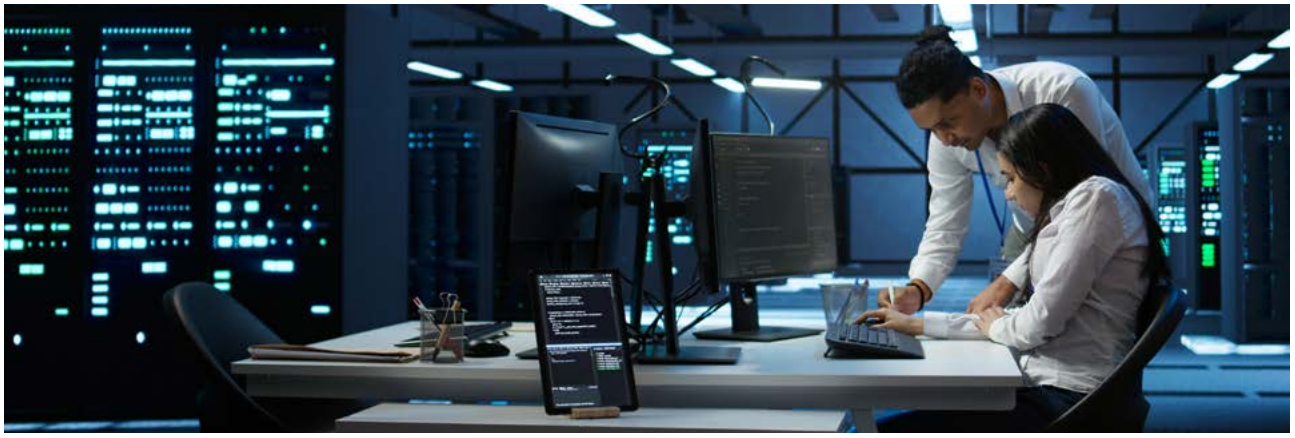
Meanwhile, London first borrowed Brussels' legal blueprint, then reshaped it for a post-Brexit regulatory landscape. The *NIS Regulations*[3] initially targeted Operators of Essential Services and a small cadre of digital service providers. That foundation will be reinforced by the forthcoming *Cyber Security and Resilience Bill,*[4] which widens the net to capture "designated critical suppliers": a sweeping category that includes large cloud operators and data-centre owners. In today's digital economy, these corporate gatekeepers control chokepoints as strategically vital as any power grids or

1 Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) [2022] OJ L333/80.

2 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).

3 Network and Information Systems Regulations 2018, SI 2018/506.

4 Cyber Security and Resilience (Network and Information Systems) Bill (HC Bill 329, 2024-26).



water networks. From a rights perspective, their stability is not a parallel concern to public infrastructure, but inseparable from the economic and civic life they underpin.

Different scripts, same play

Europe's cybersecurity policy may speak in different dialects, yet each is a defence tactfully crafted to weather the same storm. Doctrinally, Brussels's model rests on the principle of universalised resilience, treating cybersecurity as a derivative of fundamental rights and a pillar of market integrity. The *NIS2 Directive* legislates for breadth, embedding cybersecurity into the single market alongside privacy and environmental safeguards. The *Cyber Resilience Act* pushes further, setting horizontal security obligations for corporate and public operators alike under a unified defensive perimeter. Thick regulation is the norm, with harmonised, binding duties rooted in a supranational commitment to equal protection.

> **Brussels's model rests on the principle of universalised resilience, treating cybersecurity as a derivative of fundamental rights and a pillar of market integrity**

In contrast, London's post-Brexit approach prizes proportionality and targeted statutory reach. The forthcoming *Cyber Security Resilience Bill* marks a deliberate recalibration, homing in on critical fault lines that could trigger systemic disruption. This thin constitutionalism values adaptability and sectoral tailoring over, seeking just enough cross-border coherence to stay aligned with Europe's defensive baseline.

Digging deeper, the divergence is more philosophical than operational. Brussels frames resilience as the latest pillar of continental rights; London grounds its scope in the twin imperatives of public stability and economic security. Nonetheless, both rest on the same normative conviction: resilience as a constitutional obligation, not a mere technical benchmark. In both frameworks, the heaviest duties fall on the most pivotal actors whose failures could imperil the commons, because defending against amorphous threats demands the strongest shoulders.

Defending the digital commons

In Europe's tangle of cables, clouds and codes, national boundaries become a relic of defences. Brussels and London may speak in different legal vernacular, but they share the same baseline: resilience as the norm, not the exception. An underlying impulse further binds both frameworks: to

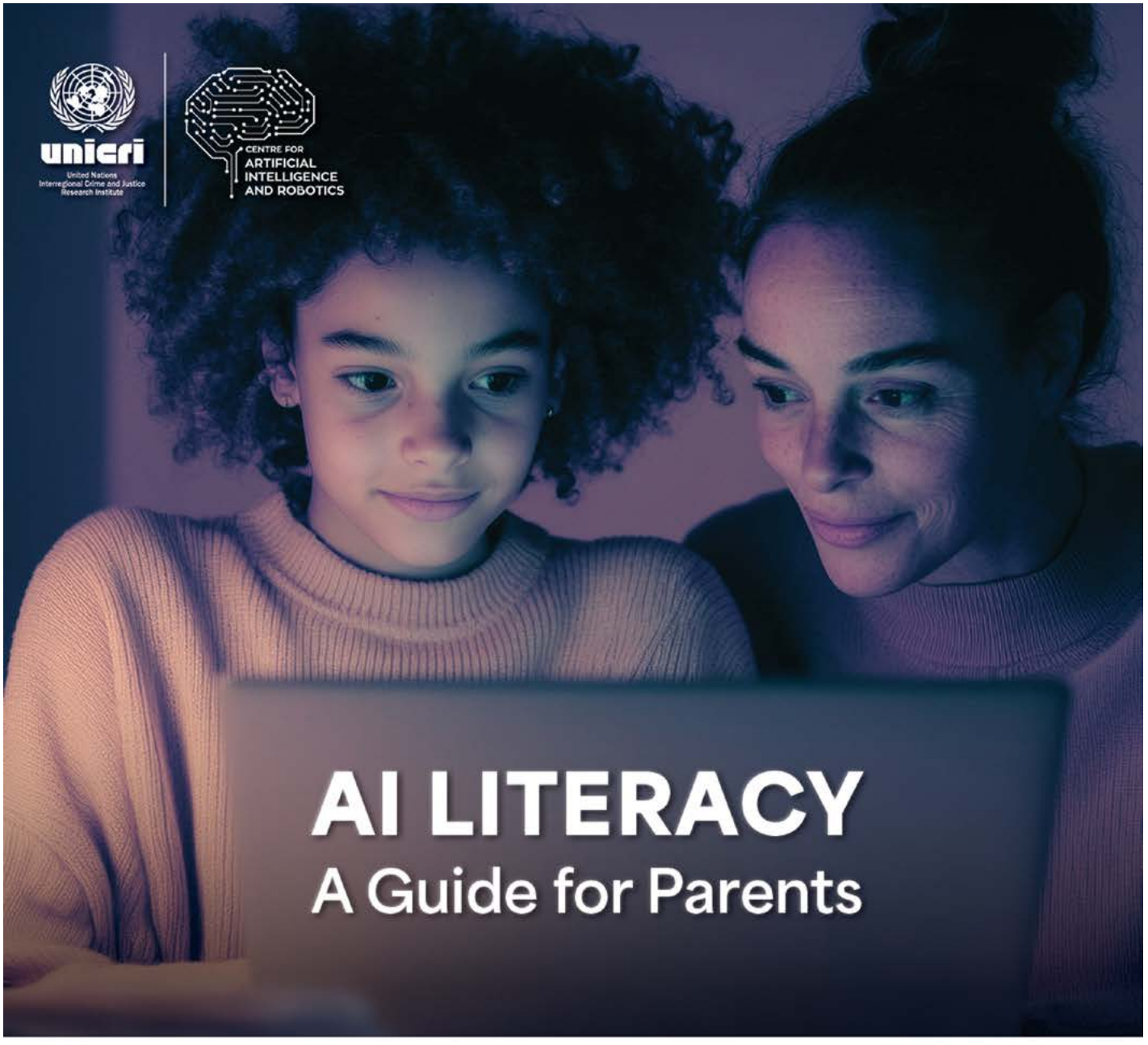
embed security deep within the arteries of public life, and to hold the most powerful actors to the heaviest duties of care.

But laws alone are fortifications without sentries: imposing on paper, porous in practice. When push comes to shove, neither Brussels' broad canopy nor London's tailored scaffolding will hold without the mortar of trust, in two senses of the word. First, interstate trust to trade intelligence when ramparts are tested, while resisting the reflex of political pride. Second, public trust in institutions to respond decisively, transparently and without deflection when cracks appear. In cybersecurity, as in diplomacy, the surest defence is not the walls nor the machinery, but the trust that stabilises it against fracture under the next shock.

Policymakers should resist treating Brussels' universalised resilience and blanket coverage as a separate track from London's targeted agility. Read together, both approaches offer complementary strengths: Brussels embeds security as a universal right, while London sharpens resources on the most consequential vulnerability. Yet, a hybrid system must confront the accompanying practical fissures: fragmented CERT-to-CERT communication, inconsistent reporting thresholds, intelligence silos that delay escalation, and the bureaucratic drag that slows real-time information sharing. A more effective course would be to shape a model that taps into the merits of both – common baseline standards, integrated supply-chain oversight, continuous joint exercises, and real-time intelligence exchanges – to stitch these defences into a system that can anticipate shocks. In the age of borderless threats, the only wrong move is to defend alone.

ABOUT THE AUTHOR

Aiko Yeo is a penultimate year LLB Law student from the London School of Economics and Political Science. As an incoming legally-trained policy analyst under Singapore's Ministry of Defence, she is committed to developing a nuanced understanding of the nexus between law, geopolitics and public policy. Aiko's academic and professional pursuits are united by a dedication to safeguarding national interests while strengthening the legal frameworks underpinning regional and global stability.


unicri
United Nations
Interregional Crime and Justice
Research Institute
CENTRE FOR
ARTIFICIAL
INTELLIGENCE
AND ROBOTICS
AI LITERACY
A Guide for Parents


unicri
United Nations
Interregional Crime and Justice
Research Institute
CENTRE FOR
ARTIFICIAL
INTELLIGENCE
AND ROBOTICS
RESPONSIBLE
AI INNOVATION IN
LAW ENFORCEMENT
AI Toolkit
Not Just Another Tool
Public Perceptions on Police Use of Artificial Intelligence
Demographic profile
of the respondents
Funded by
the European Union