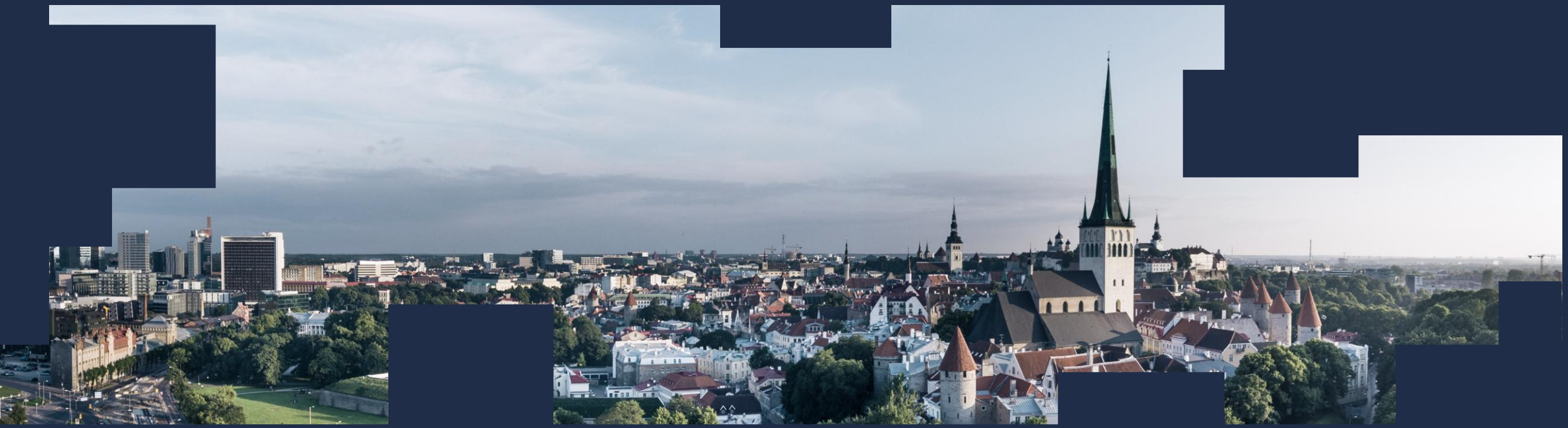
STAATLICHE RESILIENZ IM DIGITALEN ZEITALTER - die estnische Perspektive

Lilly Schmidt
Senior Consultant + Subject Matter Expert, Nortal



2007 WURDE CYBER ZU EINER NEUEN KONFLIKTDOMÄNE

Wege zu finden, um nicht nur gegen einen überlegenen Gegner zu überleben, sondern mithilfe von Technologie eine bessere und widerstandsfähigere Gesellschaft aufzubauen.

WIE KANN DIE KONTINUITÄT SICHERGESTELLT WERDEN, WENN TEILE DES STAATES ODER DER INFRASTRUKTUR ZERSTÖRT ODER BESETZT WERDEN?

Mittel finden, um mithilfe von Technologie widerstandsfähiger gegenüber physischen Störungen und Angriffen zu werden. Der „Plan B“ oder Date Embassy

WÄHREND DER PANDEMIE WAREN 30% DER REGIERUNGEN GEZWUNGEN, DEMOKRATISCHE WAHLEN ZU VERSCHIEBEN.

Doch was wäre, wenn sich alles vollständig digital abwickeln ließe?

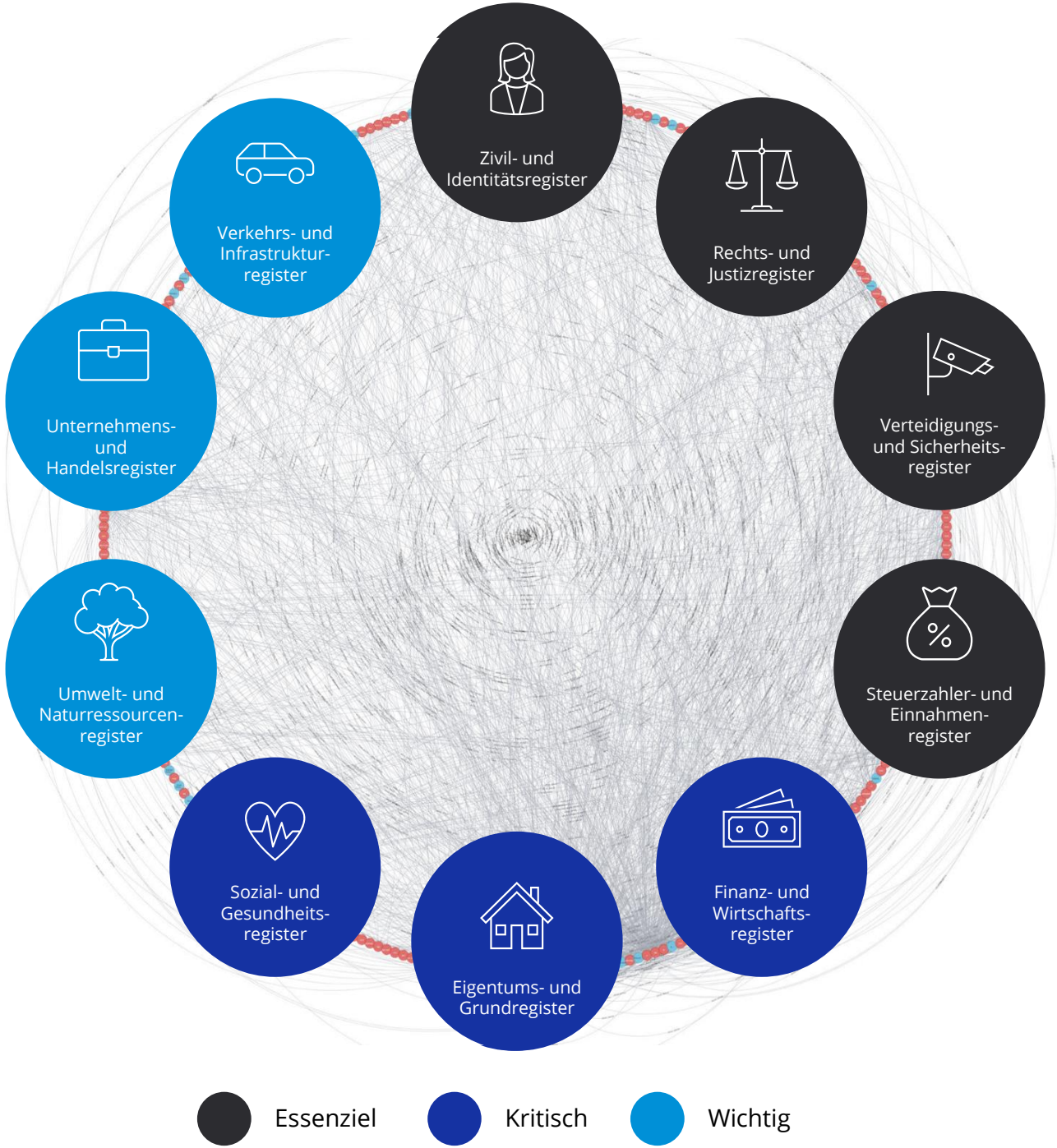
GOVERNMENT RESILIENCE IN THE DIGITAL AGE

Nortal | Estonian Government | Oxford University

PRIORITÄTEN ZUR SICHERSTELLUNG DER STAATLICHEN KONTINUITÄT IN KRISENZEITEN

Was muss im Kern geschützt werden? Kultur, Gesetze, Eigentum, Besitz- und Rechteverhältnisse

Digitalisierungsprioritäten in Friedenszeiten unterscheiden sich oft erheblich von den Digitalisierungsprioritäten, die für die langfristige Kontinuität von Staat und Nation in Krisenzeiten notwendig sind.



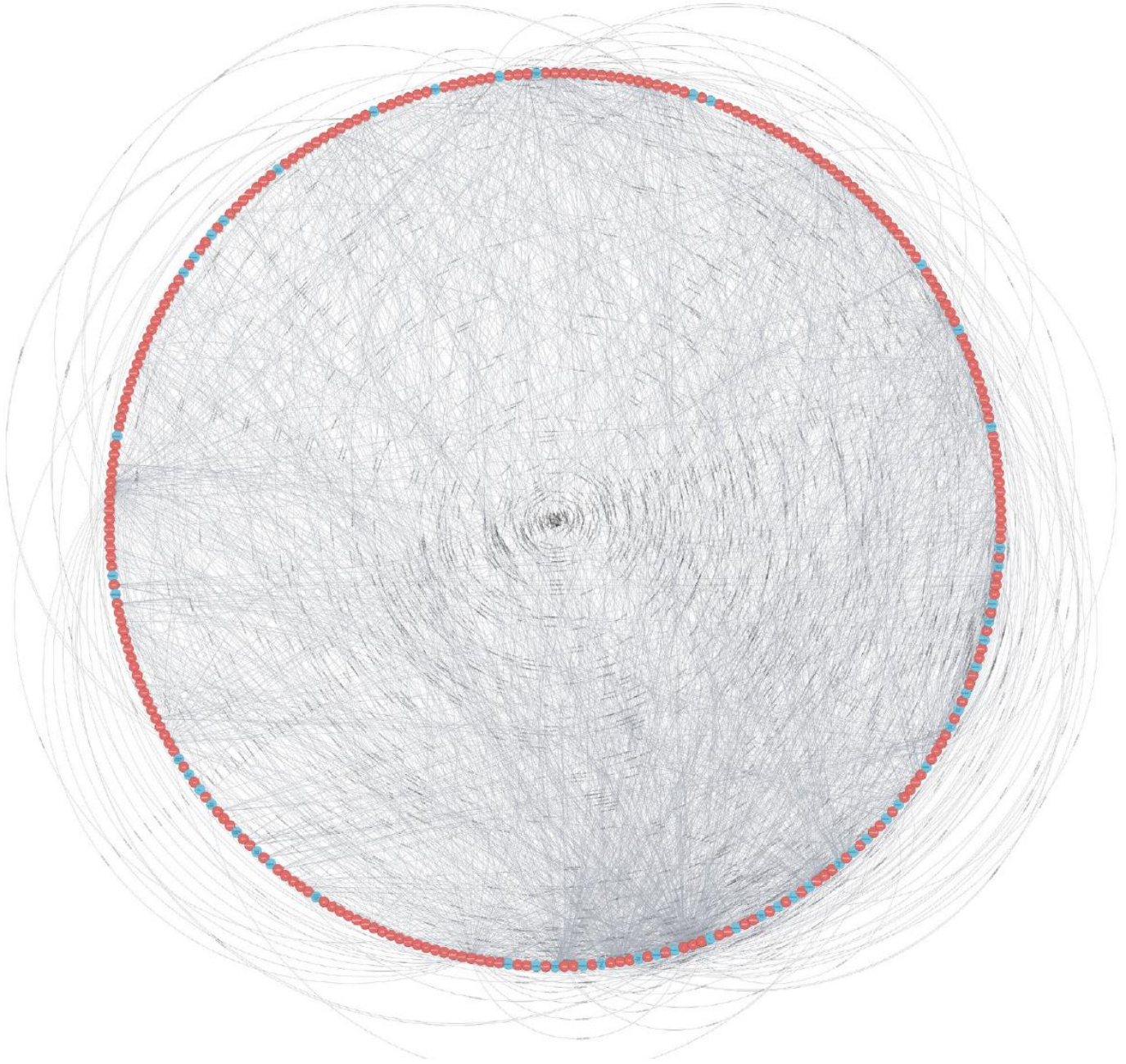
SECURE BY DESIGN AUF NATIONALER EBENE

Bestehende Systeme nachträglich so gut wie möglich absichern.

Neue Systeme so bauen, dass sie von Anfang an „by design“ angemessen sicher sind.

PKI Identifikation; Blockchain und Identifikationsmechanismen

Verbindliche Standards und praxistaugliche Architekturen



ENTKOPPLUNG DER DIGITALEN REGIERUNG VOM PHYSISCHEN STAATSGEBIET

Regierungen sind in der physischen Welt verwundbar – durch Serverräume, Rechenzentren und Single Points of Failure - langfristige Legitimitätsfragen

Phase 1: Cloud-Transition oder Duplizierung

Phase 2: Demokratien schaffen gegenseitige Safe Harbors für Teile ihrer digitalen Regierungsfunktionen.

Größte Hürde: Regulatorik

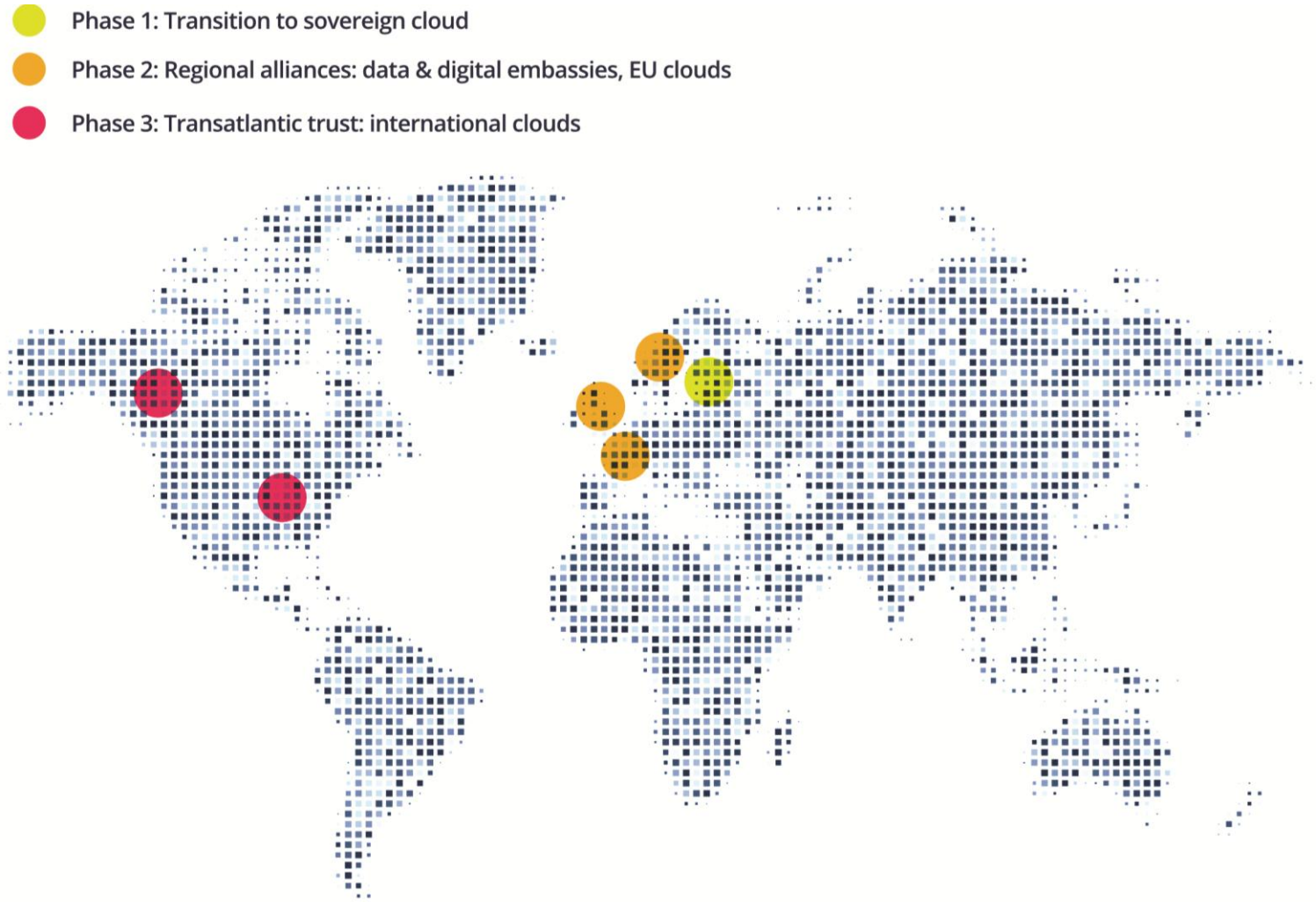


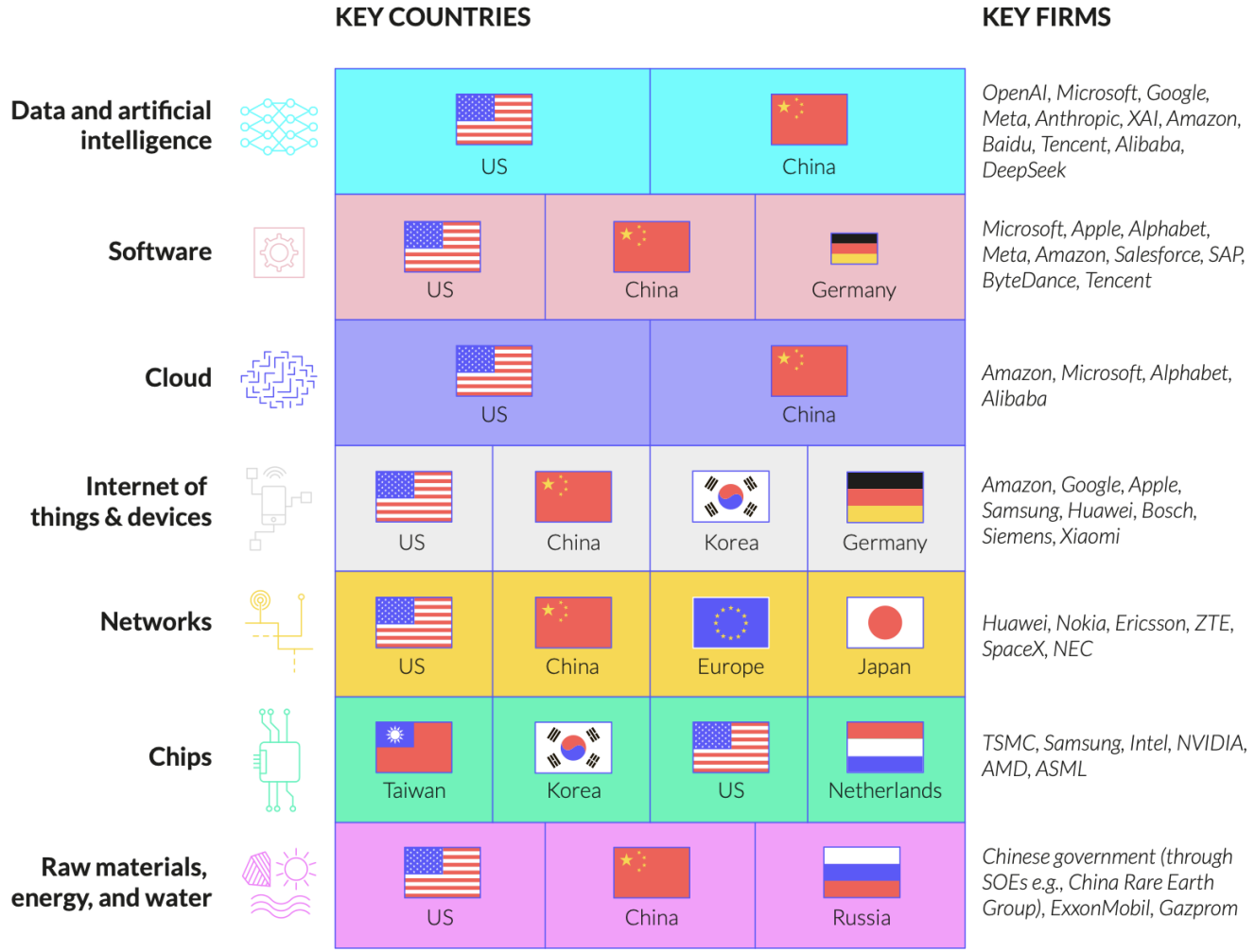
Figure: Phased transition to wider international alliances based on mutual trust and agreements. The locations on the map are for illustrative purposes only.

DIGITALE SOUVERÄNITÄT IST ZU EINER KRITISCHEN SICHERHEITSKOMPETENZ GEWORDEN

Für nationale Sicherheit und Souveränität ist entscheidend, wem die Technologien gehören, auf denen staatliche Handlungsfähigkeit basiert.

In Estland wurde deshalb früh darauf gesetzt, die digitale Zukunft nicht ausschließlich von US-Unternehmen bestimmen zu lassen.

Open Source: Durch die intensive Aufmerksamkeit aus Russland gab es über Jahre hinweg eine Art „unfreiwilliges, kostenloses Penetration Testing“.



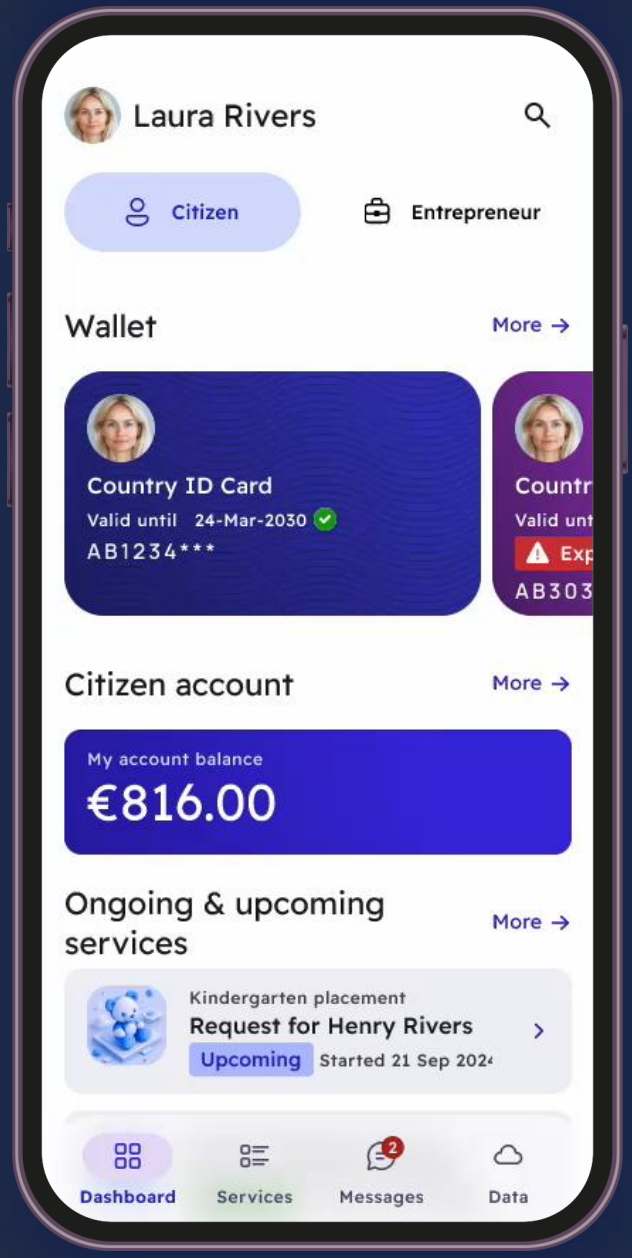
EuroStack report 2025

REMOTE FIRST IM ÖFFENTLICHEN SEKTOR

Natürlich kann die Resilienz von Staaten deutlich steigen, wenn Bürgerinnen und Bürger kritische Leistungen digital und aus der Ferne nutzen können. Aber häufig wird dabei die andere Seite vergessen: die Menschen, die diese Leistungen überhaupt betreiben – die Beschäftigten im öffentlichen Dienst. Auch sie sind in Krisen genauso betroffen wie die Bevölkerung. Wenn Bürgerinnen und Bürger nicht nach draußen können oder remote arbeiten müssen, gilt das auch für Verwaltungsmitarbeitende.

Beschäftigte im öffentlichen Sektor sind in Krisen ebenso verwundbar wie Bürgerinnen und Bürger.

WIE SIEHT STAATLICHE RESILIENT FÜR ESTLAND AUS?



Digitales ist der primäre Kanal für die Leistungserbringung: 100 % digitale, unterbrechungsfreie Bürgerservices

Beschäftigte des öffentlichen Sektors sind befähigt, ortsunabhängig zu arbeiten

Digitale öffentliche Infrastruktur ist Secure by Design

Keine Single Points of Failure: Daten und physische Infrastruktur können nicht physisch zerstört werden

Internetzugang ist flächendeckend, kostengünstig und jederzeit verfügbar

Oxford Internet Institute
University of Oxford
Republic of Estonia
Ministry of Economic Affairs and Communications
rit Estonian IT Centre
Nortal

Vielen Dank!

Resilient ~ digital-first + sovereign