Digital Sovereignty What needs to be done

Mr. Mike Gaertner

CEO/CTO

Cambodian Network Exchange

Digital sovereignty means that We control our own service delivery, ensuring that our critical data and essential digital functions are governed by national law and remain operational, regardless of foreign technological or geopolitical events.

Breaking ... bad

What went wrong in 2024/2025

Microsoft Global Outage (CrowdStrike)

- **Date:** Evening of **Friday, July 19, 2024**.
- **Effect:** A faulty software update from the cybersecurity firm CrowdStrike caused a widespread global disruption of **Microsoft Windows systems** (the infamous "Blue Screen of Death" - BSOD). While general internet was up, any enterprise or government service in Cambodia relying on globally patched Windows systems (e.g., for terminals, internal network infrastructure) have faced operational shutdowns, system crashes, and service interruptions.
- **Major Risk:** Reliance on a single global software vendor's automatic updates can lead to a supply chain failure that cripples local operations using that software.

Internet Link Disconnection with Thailand

- **Date:** Effective **Midnight, June 13, 2025** (Announced June 12, 2025).
- **Effect:** Major telecom and IPS operators had to swiftly **re-route all international IP transit routes** away from Thailand due to a government decision following border tensions. This transition caused **temporary internet slowdowns and service disruptions** for mobile, home, and enterprise users across the country as traffic shifted to alternative gateways (via Vietnam and Laos).
- **Major Risk:** A geopolitical decision can instantly sever a major, relied-upon connectivity route, causing immediate service degradation for overseas-dependent services.

AWS Global outage (October)

- **Date: October 20, 2025**.
- **Effect:** A significant global outage in a critical AWS region (initially US-East-1) caused a widespread failure in DNS management, leading to **113 AWS services stopping work** and impacting a vast list of globally hosted websites and applications (e.g., Snapchat, Zoom, Canva). Services in Cambodia that rely on these globally available platforms or on AWS for their own hosting have experienced **inability to connect/load** for hours.
- **Major Risk:** Even with local redundancy, a flaw in a *shared global subsystem* (like DNS) in a major cloud provider creates a single point of failure for all dependent services, regardless of where the end-users are

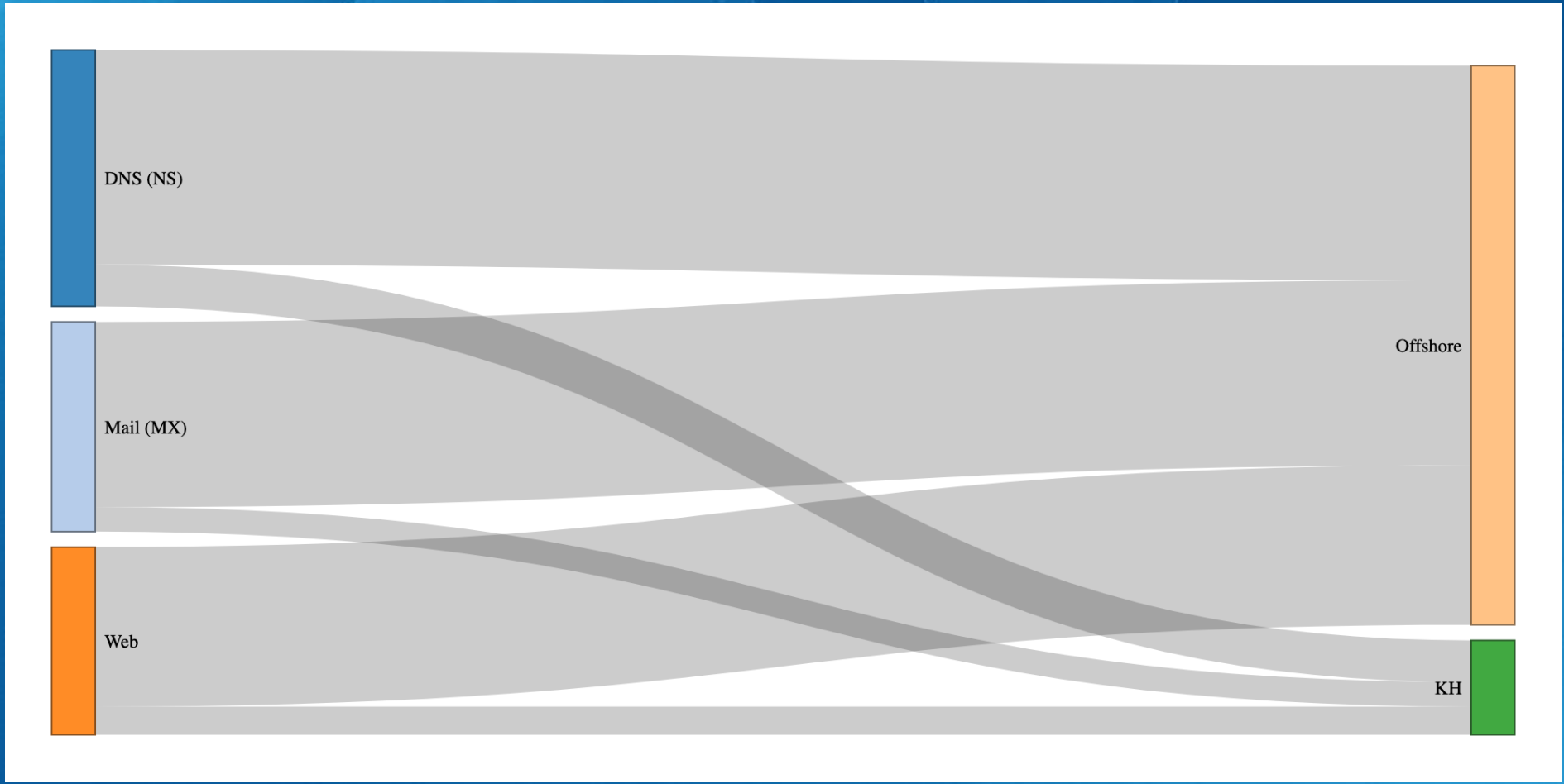
Cloudflare Global Outage (November)

- **Date: November 18, 2025**.
- **Effect:** A software bug in Cloudflare's Bot Management system caused a 3-hour global outage that knocked out access to major websites and services worldwide, including banking service for Cambodia. Many sites that use Cloudflare for performance and security have displayed **error messages** or been inaccessible in Cambodia.
- **Major Risk:** Reliance on a Content Delivery Network (CDN) or DDoS protection service, even a highly reliable one, means a bug in their system can instantly block a large portion of the global internet, including any Cambodian service that relies on it.

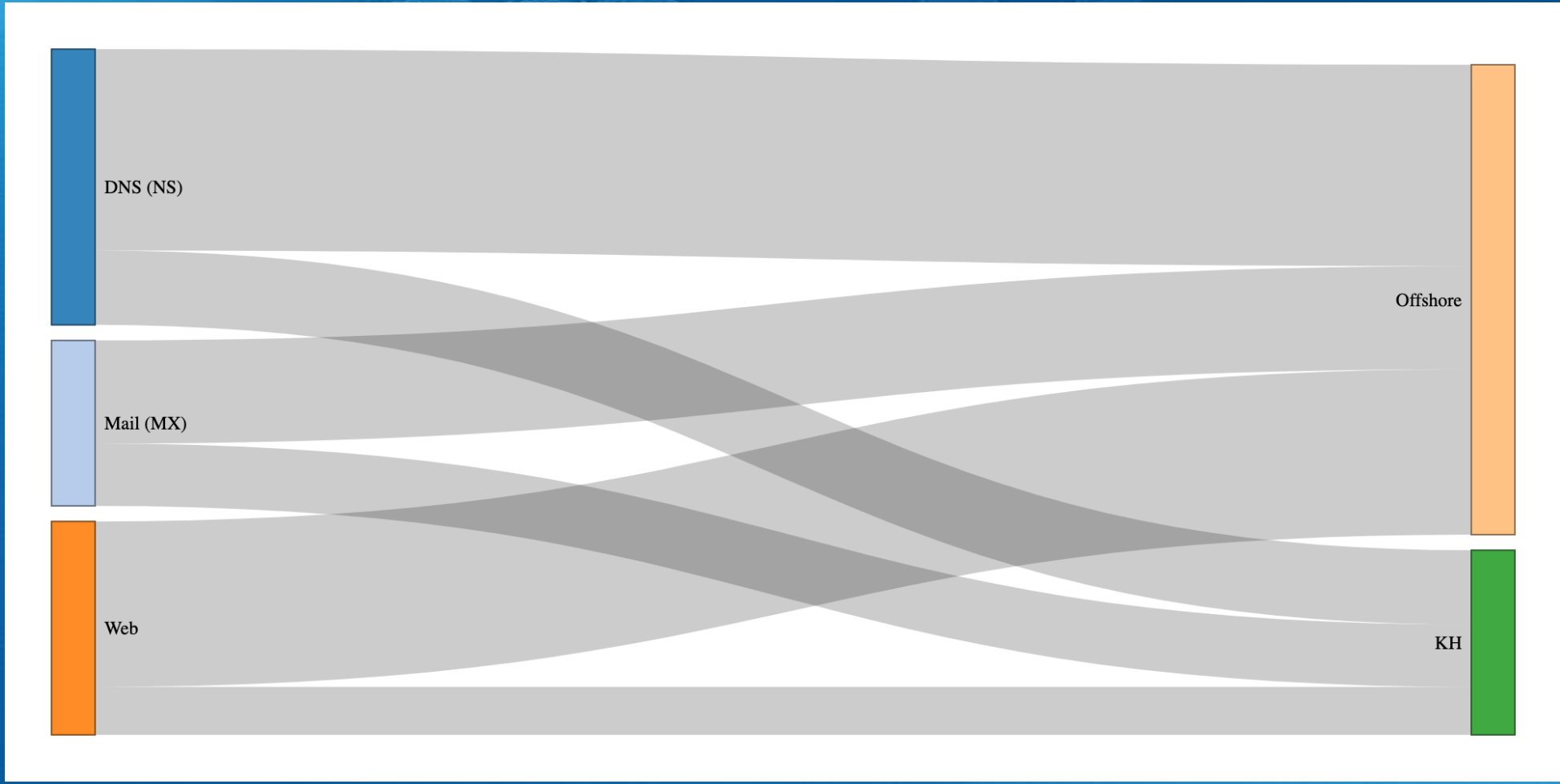
So where are we ?

Geolocation of services based on IP addresses as found in DNS records

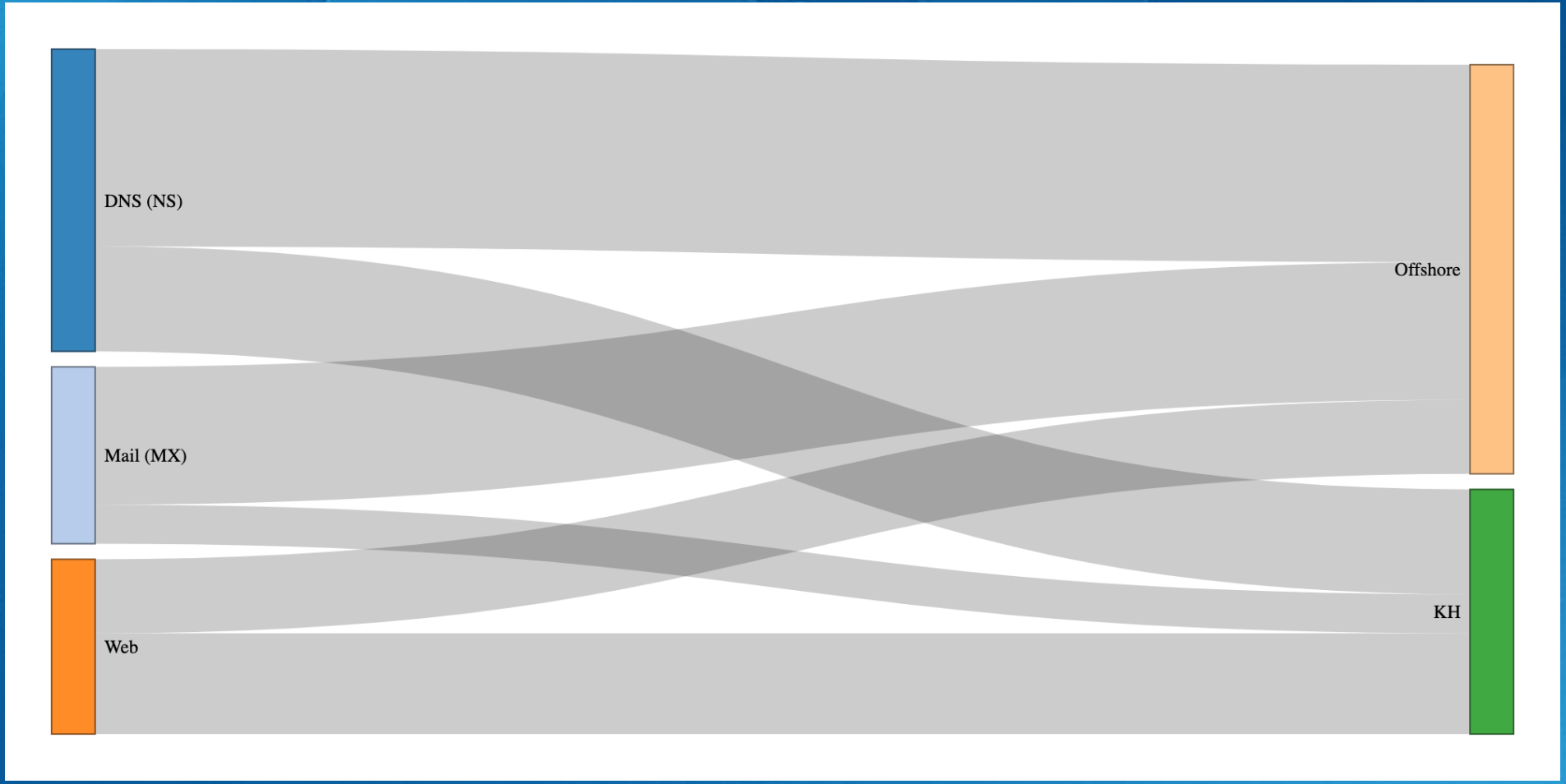
Banks dependencies on offshore hosting



Government dependency on offshore hosting



ISPs, DCs dependency on offshore hosting



What where how

Lets start our journey!

The Chain of Digital Sovereignty

Part I moving data

- **Hardware & Infrastructure** — the physical cables, routers, and switches where control begins.
- **Routing & Addressing** — who defines our networks and validates our paths.
- **Naming & Trust Anchors** — DNS, DNSSEC, and the identity roots of our digital presence.
- **Time & Synchronization** — the clock that makes every transaction and audit credible.

Part II working with data

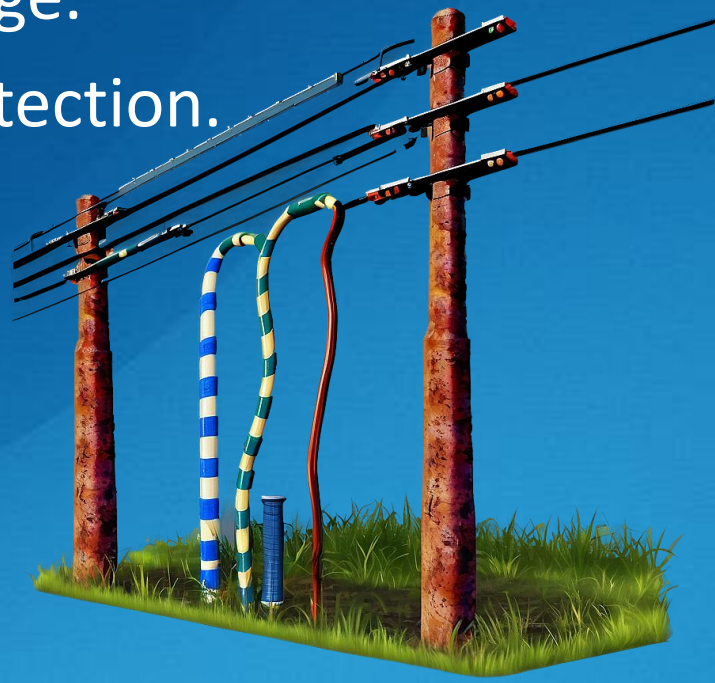
- **Identity & Access** — who authenticates our users and services.
- **Operation & Supply Chain** — the code, updates, and platforms we rely on.
- **Data Storage & Protection** — where information lives, who can access it, and under what law.

Physical Layer — "The Wires & Waves"

- Every bit of data rides on **physical infrastructure**
- Submarine cables, terrestrial fiber, towers, IXPs, and data centers.
- Routers (CPE, CE, Core), switches, OLTs, and transceivers the machines that move every bit.
- The **national IXP and data centers** form the first point of sovereign control.
- ISP connecting users to infra
- Inside Cambodia, they define what's truly under national control.

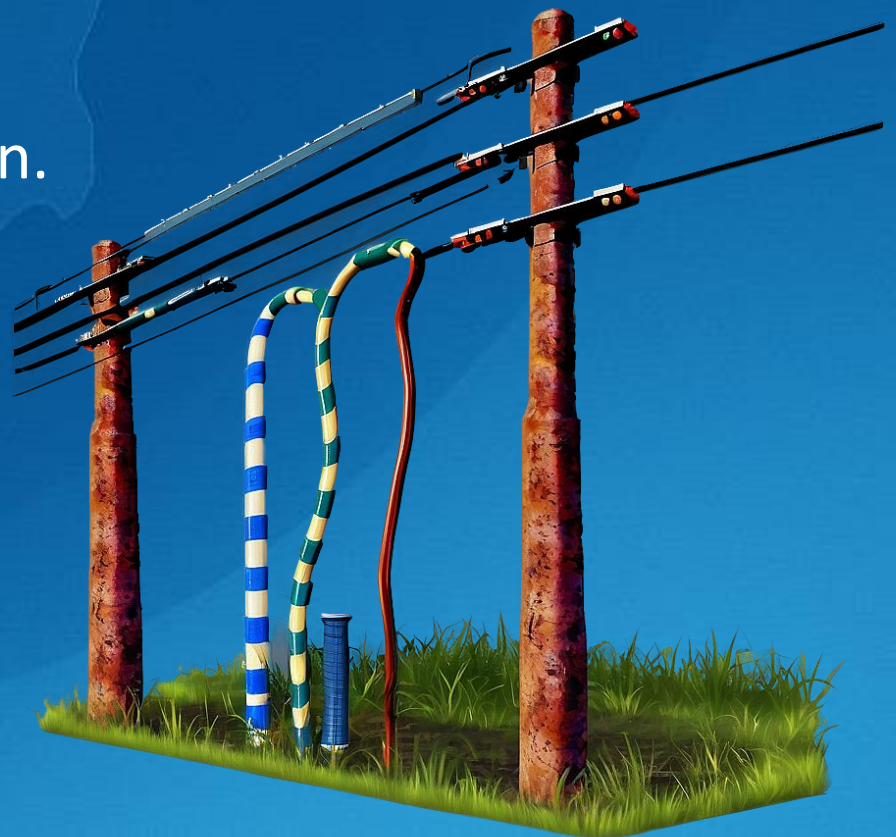
Control the Wire, Control the Flow

- **Throttle it** → Control the speed of information and commerce.
- **Monitor it** → Visibility into every unencrypted packet.
- **Permit or deny** → Decide which networks connect at all.
- **Replace it** → Supply chain control = long-term leverage.
- **Reprogram it** → Redirect or mirror traffic without detection.



Physical Layer — where we can act

- **Adopt open-network operating systems** (SONiC, Cumulus, FRR) — software-defined, vendor-neutral, auditable.
- **Promote open hardware standards** — OCP-compliant switches, white-box routers, locally serviceable OLTs.
- **Foster a diverse vendor ecosystem** — avoid single-country supply chains and proprietary lock-in.
- **Train local engineers** — enable domestic maintenance, firmware signing, and security validation.
- **Support regional manufacturing and assembly** — routers (CPE) and optics built or configured under Cambodian oversight.



Network Layer — "Who Carries our Packets?"

Routing — The Map of the Internet

- Routing decides how packets travel between networks.
- The Border Gateway Protocol (BGP) exchanges paths between ISPs, data centers, and cloud providers.
- It defines which path your data takes — domestic or abroad.
- Without routing, there is no communication between networks.

Network Layer — Control Points in Routing

- **IP Addresses** — Allocated by **APNIC**, the regional Internet registry for Asia-Pacific. Ownership gives the right to publish routes, but the *ultimate authority* remains under APNIC policy and infrastructure.
- **Autonomous System Numbers (ASNs)** — Also issued by APNIC; define the identity of each network in BGP. Without a valid ASN, a network cannot participate in the global network.
- **RPKI & ROA** — Cryptographic route validation keys hosted and signed within APNIC's trust anchor. If APNIC revokes or loses control, local validation collapses.
- **Local BGP Policy** — Domestic route servers (e.g. at CNX) can enforce local preference, but depend on APNIC-rooted data for legitimacy

Dependency Reality — These functions are *regional by design*; sovereignty here means **visibility and participation**, not isolation.

Network Layer — Control the Routes

- **Hijack it** → Announce another network's IPs; steal traffic.
- **Silence it** → Withdraw prefixes; make entire services vanish.
- **Observe it** → Force routing through foreign jurisdictions.
- **Delay or degrade** → Shape the national user experience.

Network Layer — what we should care for

- **Promote local ASN ownership** — ensure every bank, telco, and ministry holds its own AS number.
- **Keep things local!**
- **Deploy national RPKI infrastructure** — hosted under Cambodian jurisdiction.
- **Advance IPv6 adoption** — eliminate dependency on scarce, leased IPv4 from foreign brokers.
- **Educate engineers** — operational security, ROA management, and path validation.

Naming & Addressing — "How we Finds Things"

- The Domain Name System (DNS) translates names to IP addresses.
- Root DNS server delegate names to owners (.kh);
- Authoritative DNS defines *who owns* a name; (cnx.net.kh)
- Resolvers talk to AuthDNS to tell the user *where it goes*.
- DNSSEC adds cryptographic trust to prevent tampering.

Every website, app, and API request begins with a DNS lookup.

Naming & Addressing — Root, Registry & Resolvers

- **Root Zone** — managed globally by **ICANN /IANA**; Cambodia's .kh depends on that root chain.
- **.KH Registry** — operated under TRC policy; authoritative servers determine visibility of every Cambodian domain. Registry servers delegate to owners
- **Authoritative DNS Hosting** — actual domain data (web, email, api, security setting DANE, CAA) often outsourced abroad;
- **DNSSEC Trust Anchor** — anchored in the global ICANN root; local keys validate beneath it (not implemented in .KH)
- **Dependency Awareness** — Cambodia's namespace lives inside the global root trust — participation ensures resilience; ignorance risks invisibility

Jurisdiction follows the host, not the domain owner.

Control the Names, Control the Trust

- **Redirect it** → Point .kh traffic to any server, anywhere.
- **Block it** → Make entire ministries or banks vanish from the internet.
- **Impersonate it** → Forge DNS data and obtain “valid” SSL certificates.
- **Exploit it** → Control over names equals control over identity.

Naming & Addressing – how to improve

- **Recognize DNS as national critical infrastructure.**
- **Enable DNSSEC for .kh** — sign all zones with HSM-protected keys under Cambodian jurisdiction.
- **Host DNS root servers in-country** — expand deployments , leading are CNX, Mekong Net, and Neocom.
- **Operate trusted public DNS infrastructure** — offer both **authoritative DNS hosting** (CNX Anycast) and **secure public resolvers** for national use (quad9).
- **Reduce foreign dependence** — understand which .kh domains resolve abroad and define clear guidelines for local accessibility.
- **Engage globally** — participate actively with ICANN and APNIC to maintain visibility while strengthening local resilience.

Identity & Trust Anchors — "Who am I talking to?"

- Every "secure" connection depends on digital certificates to get a "secure" status.
- Certificates are issued by **Commercial Certificate Authorities (CAs)** — a global industry of more than 400 organizations.
- CAs can revoke certificates at any moment, without any warning
- The result: services depend on trust lists maintained by U.S. and EU corporations.
- Certificates confirm only **domain control**, not organizational identity or jurisdiction

Browser and OS vendors decide which CAs are trusted by default *not* national regulators or service owners.

Identity & Trust – Control and Consequences

- **Anyone controlling DNS** can pass CA domain-validation challenges → obtain “valid” certificates for any domain.
- **Browser control** determines whose certificates appear “secure.”
- **Foreign revocation policies** can remove access to Cambodian services without local oversight.
- **DNSSEC + DANE** (DNS-based Authentication of Named Entities) could provide verifiable, cryptographic binding between domain and certificate — but remain largely unused because browsers ignore it.

Real identity is absent
TLS proves encryption, not ownership.

Identity & Trust — the next step

- This is a big one, we need to fundamentally shift the trust model we use to identify and trust servers
- **Nation states need to work with browser vendors and ICANN** to recognize DNS-anchored identity as a trusted model.
- **Use DNSSEC as the root of identity** — publish and verify certificates directly via DANE/TLSA records.
- **Develop a national CA and PKI policy** — managed under Cambodian jurisdiction, aligned with DNSSEC chain of trust.
- Till that is done, monitor certificate issuance!

Time & Synchronization — "When Events Happen"

- Every transaction, log entry, and cryptographic signature depends on accurate time.
- Banking audits, security events, and digital forensics all start with timestamps.
- Most systems synchronize from **foreign NTP sources**, usually unauthenticated and unverifiable.
- Cambodia's auditability and cyber resilience depend on **trusted, in-country time**.

Securing the Clock

- **Establish a national reference clock** — combine GPS, BeiDou, and Rubidium sources.
- **Deliver time over the domestic network** — PTPv2 for precision, NTP with NTS for authentication.
- **Integrate with regulated sectors** — banks, ministries, and telecoms synchronize under Cambodian jurisdiction.

Whoever sets the clock defines the truth in every log, every transaction, every audit.

That was the journey of data being moved, now lets add some use to it

This is a massive undertaking and it will always have unresolvable dependencies, but we need to evaluate them, understand them and find the best middle ground. A lot in the next slide is a direct overlap with what you know from cybersecurity best practice, now add the jurisdiction component.

Beyond the Pipe — Where Data Lives

- Once data reaches the service, sovereignty depends on how we:
  - **Identify** — who owns it and who gets access.
  - **Operate** — the systems and dependencies we use to work with it.
  - **Store** it — where and under which jurisdiction.
  - **Protect** it — against loss, interception, or misuse.
- Each of these functions relies on global vendors, update feeds, and identity frameworks that may lie beyond Cambodia's legal reach.
- **Securing these systems defines operational digital sovereignty.**

Identity — Building better systems

- **Anchor service identity in DNS:** DNSSEC + DANE (TLSA) to bind certs to names under .kh. (remember we have a real hard time established service authenticity!)
- **National or sectoral federated IdP:** Local IdP(s) using OpenID Connect / SAML with strict issuance & audit rules.
- **Run PKI and key material domestically:** CA keys in HSMs with multi-site custody and audits.

Identity equals control of sessions, services, data and recovery paths not just usernames and passwords.

Operations — The Opportunity

- **Mirror critical repositories locally** — OS updates, container images, and CVE feeds hosted under Cambodian jurisdiction.
- **Promote reproducible builds & code signing** — verify what's compiled matches reviewed source.
- **Adopt open platforms** — Linux, Kubernetes, OpenStack — that can run anywhere, audited by local engineers.
- **Establish national build and signing infrastructure** — HSM-protected keys, auditable pipelines.
- **Foster secure development culture** — SBOM (Software Bill of Materials), static analysis, mandatory patch transparency.
- **Collaborate regionally** — mirror and verify upstream packages within ASEAN

Our operational sovereignty today depends on update servers, certificate authorities, and repositories we do not own or govern.

Keep Critical Data Within Reach and Under Law

- **Host regulated data in-country** — domestic data centers under Cambodian jurisdiction.
- **Separate data and key custody** — keep encryption keys in local HSMs or sovereign key management systems.
- **Mandate lawful-access transparency** — providers must disclose foreign data-request channels.
- **Promote hybrid models** — public cloud for scale, domestic cloud for control.
- **Adopt open storage platforms** — Ceph, MinIO, OpenStack Swift — auditable, vendor-neutral.
- **Define "critical data classes"** — banking, citizen records, national platforms — must remain within Cambodia

"The Cloud" is just ***someone else's data center***
physical servers are governed by the law of their location.

Security Inside the Border

- **Build domestic SOC capability** — monitoring and incident response under Cambodian law.
- **Keep decryption local** — terminate TLS inside sovereign networks; share only anonymized indicators.
- **Use open or locally hosted tools** — Suricata, Zeek, Wazuh, OpenWAF, ELK Stack.
- **Mandate data-handling transparency** — security vendors must declare where logs and telemetry are processed.
- **Establish national threat-intel exchange** —privacy-preserving, no data exfiltration.
- **Train local analysts** — skill development to replace "black-box" managed security.

True defense means protecting the data — not exporting it for someone else to study.

We can do it

- No nation starts digitally sovereign — it's achieved one system, one standard, one collaboration at a time.
- The dependencies we face today are not failures — they are *maps* showing where we must act.
- Every domestic node, mirror, key, and policy strengthens our independence.
- Cooperation between **government, industry, and engineers** can transform vulnerability into capability.
- The future is within reach — we already have the people, the networks, and the vision.

YOU can make a difference

Just start somewhere

Thank you

gaertner.mike@cnx.net.kh