The World Wide Web Stress Test

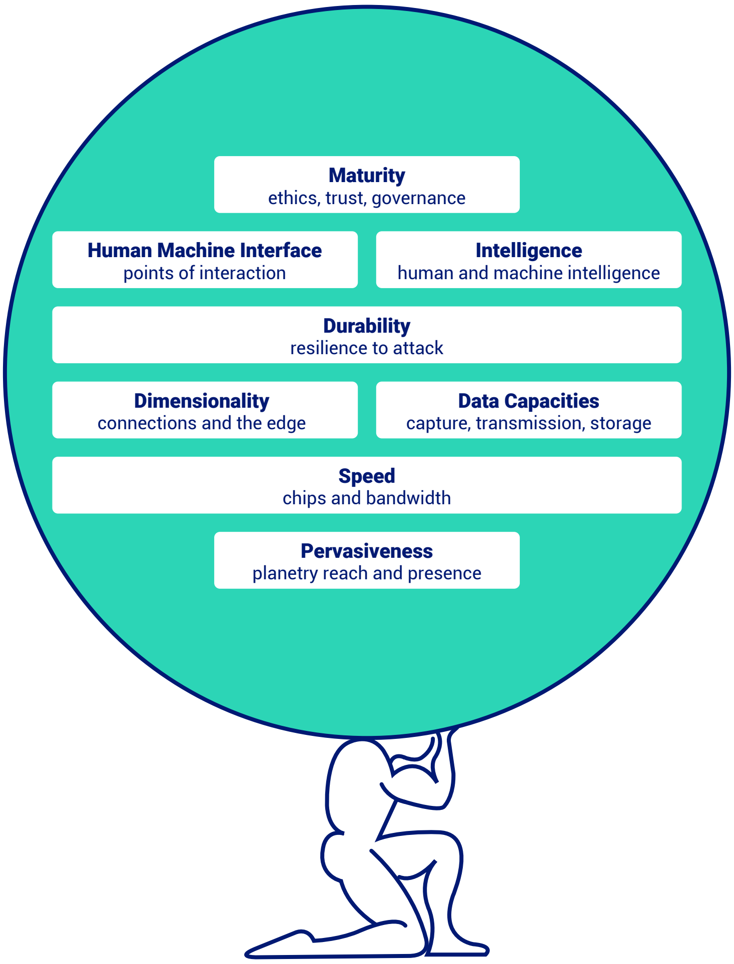
Debra Bordignon, SVP Strategy, Innovation and Technology, NTT Ltd. Australia

Our Digital Earth and Heavens

The internet is like the Atlas statue, holding up our digital earth and heavens on it's shoulders. This is core infrastructure for our current and future world and at 31 years if age, the internet might need more than some strength training to continue to hold us up. It may be near breaking point, heralding a paradigm shift.

There is an unprecedented experiment underway. This is a big deal, possibly the biggest deal of all in the medium term for digital transformation. There are technology principles, laws, and models about each of the dimensions making the internet functional. Modelling assumptions never included an event causing the whole world to be simultaneously living, learning, working and trading online. The post pandemic new normal will not see the spike fully recede and the trajectory will follow an increased exponential factor.

Coverage of the question of 'how is the internet performing during the crisis?' centres almost entirely on bandwidth performance. Yet the internet is more than bandwidth and connection nodes. There are eight dimensions of the internet. Think of this anatomically. The skeletal dimensions are the pervasiveness and the speed of the internet. Physiological dimensions are dimensionality, data capacities and durability. Cerebral dimensions are the human machine interface and intelligence and the highest order dimension is maturity. The stress test is impacting all of these dimensions, but most tellingly, the first five dimensions and ultimately, the issue of maturity.



Dimensions of the Internet (adapted from Thomas Frey, Futurist)

Pervasiveness - Planetary Reach and Presence

According to our world in data, the number of internet users grew from 413 million in 2000 to over 3.4 billion in 2016. Coming into 2020, there were 4.5 bn active users, around 59% of the global population. Of the 3.6 bn people who remain totally offline, the vast majority are from developing countries. The current planetary broadband coverage is just 44%.

In normal times, around 640,000 users go online for the first time every day. Models predicted 5.1 bn users by 2025. A whopping 72% of these users will only access the internet via their mobile device – underlining the United Nations Broadband Commission point that this pandemic has underscored the vital importance of broadband infrastructure to governments and communities around the world.

In affluent countries, grandparents and school students are logging on for the first time at greater cadence and many small businesses are also moving to e-commerce for the first time. Yet in developing countries, where most of the world's 1.5 bn school children live, broadband coverage is not pervasive and quality is often as low as 2G bandwidth. These people lack vital information about the pandemic and are put at far greater risk.

So, the overall surge in connected nodes has increased the already unacceptable inequities between the digital haves and have nots. Indeed there's a growing movement including the United Nations, calling for internet access to be declared a protected human right, offered at no cost and not traded as a luxury product.

Post pandemic, we will surely see public-private and philanthropic partnerships expand to complete the planetary roll out of internet access. But, assuming we are all connected by 2025, we'll be competing with 9 bn other users and 41bn Internet of Things devices for bandwidth, which is currently finite. This makes 5G imperative in the very near term for our post COVID society and economy.

But it's also imperative to explore solutions beyond the current spectrum and technology paradigms. Which leads to the next dimension.

Speed – Bandwidth and Chips

Countries differ, based on their lockdown polices, but Forbes estimate demand for bandwidth has increased by ranges of 50% to 70% generally, and as high as 90% in complete lockdown situations. Internet speed and resilience has plunged in every country, regardless of whether 3G, 4G or 5G enabled. Some services providers (such as the video streaming platforms) have taken steps to throttle quality to retain acceptable latency, Governments have instructed Telcos to prioritise critical business access, and in some countries, citizens have been locked out of internet access.

Internet speed is governed by Neilsen's Law, which states that that network connection speeds for high-end home users increase by 50% each year. This anticipates multi-faceted changes such as - growth in users, the shift fom 3G to 4G and 5G, 5Gs wireless enablement of the Industrial Internet of Things with many billions more connected things, machine to machine communications, data volume increases, the shift toward distributed computing, increased edge storage and computational capacity, richer interfaces like Virtual Reality and growth in digital twinning databases. Clearly, the accrued demand requires exponential growth in internet speed.

The pre-pandemic models predicted that available broadband would be exhausted by 2035, and it is widely accepted that the current Radio Frequency (RF) spectrum is not sufficient to future-proof wireless communications. The modelling curve is now accelerated by COVID, almost certainly the 2035 prediction will be brought forward, perhaps by as much as a decade. Hence, due to this looming RF crunch, there is growing interest in using the optical spectrum for wireless communications.

Since 1965, computer speed has been governed by Moore's Law, which states that every two years will see a doubling in the number of transistors that can be fitted into a single integrated electronic circuit (chip). This has guided digital electronic advances, but Moore himself expects the exponentials of the law to end by around 2025.

Moving forward, chip development will be driven by applications requirements. Emergent applications like digital twinning, AI, virtual reality, biological sensing and quantum analytics, require a shift from the classical computing paradigm. Photonic (optical) circuits are fast evolving to process these application use cases. Photonic computing uses the optical wireless spectrum, consumes less energy than electronic circuits, computes exponentially faster at terabytes per second and is non-binary, capable of multiple simultaneous processes.

Underscoring the importance of photonics for the next era of internet and cloud services evolution, NTT, Intel and Sony have founded a global forum, called IOWN (Innovative Optical Wireless Network). With NTTs heritage in photonic related R&D fields and by combining each partners respective strengths in networking and AI, integrated circuits and smart devices, this collaboration aims to bring forward the paradigm shift to distributed connected computing, edge computing, high performance computing, powered by converged electronic – photonic and all photonic infrastructures. This is a vitally necessary paradigm shift.

> Underscoring the importance of photonics for the next era of internet and cloud services evolution, **NTT, Intel and Sony have founded a global forum, called IOWN (Innovative Optical Wireless Network).**

Data Capacities and Dimensionality – Connections and the Edge, Data Capture, Transmission and Storage

In late 2019, IDC predicted that data volumes were growing at 28.7% annually and would reach 175 zettabytes by 2025, with 49% living in public cloud. One third of all data will be processed at the edge, by intelligent sensors and devices. The Internet of Things will account for 90 zettabytes of data, flowing from 41.6 billion nodes. One third of all data will be processed real time. Around 2025, when Industrial Internet of Things systems are mature and scaled, data growth rates will be beyond exponential.

During the pandemic lockdowns, a massive uptick in data volumes has occurred, related to video content streaming, but also video chat / conferencing and ecommerce activity. The volume and nature of telemetry and big data being captured, transmitted and stored has morphed - previously unseen amounts of real time big data related to the pandemic is streaming in at high velocity to feed analysis engines. There has not been a time before where so much real time data monitoring and analytics has occurred. Given the co-dependencies between data, broadband speed and computation capacity, this surge in data also emphasises the need for evolving models and technologies across these dimensions. Data-centric computing and storage that ensures good governance of data across it's lifecycle is a key priority, to ensure the competitive, social and historical value of data can be realised.

Durability – Resilience to Attack

ICANN (The Internet Corporation for Assigned Names and Numbers) co-ordinates the internet's address book, the Domain Name System (DNS). In Feb 2019 ICANN warned the world of ongoing and significant attacks on the core infrastructure of the internet, the DNS, and that this is an imminent threat to the secure function of the internet. ICANN pointed to a growing pattern of attacks using different techniques in order to hijack traffic through DNS modifications and compromises. These threats come from well resourced and sophisticated criminal empires and state-based actors.

The global DNS infrastructure and protocols were conceived in linear times, before the explosion of mobility, social, cloud services and the consequent extent of digital activity. Several fundamentals of the DNS are evolving, yet grapple with durability in rapidly changing times.

Data sovereignty is one of these fundamentals. Now that over 40% of all data lives on cloud services, data sovereignty is a hugely important and often contentious issue. Maturity is low, there is a lack of global standards, governance and regulation. Unless you are the USA, your country's data assets are likely to be hosted under another country's domain extension. This gives rise to sovereignty conflicts, including citizen data protection, IP ownership, research and data trading rights and individual data rights. Governments are nevertheless asking citizens to share their data at scale, to help combat the spread of the virus. Generally speaking, citizens are sharing for the greater good, but no one, including governments, can in reality assure citizens about their data safety and rights.

Another fundamental is cyber security. DNS requests are what flow data, from inside to outside an organisation, from party to party. DNS requests create openings in firewalls, they are the weakest innate link and therefore biggest hack target in an organisation's security architecture.

To combat the horrors of growing cyber attacks, Governments have collaborated with ISPs to develop intrusion prevention that identifies and blocks cyber attacks. The latest evolution is Einstein 3 Accelerated, E3A. In the USA, the ISPs provide intrusion protection capabilities as Managed Security Services. Information is aggregated across government agencies to form complete insights of activity and interventions are rapidly shared across the networked eco-system.

China has implemented a national network security strategic plan based on E3A, building situational awareness and autonomous action to control DNS activity. They are criticised for also using this undemocratically, to monitor and control citizens access to information. Ruggedisation of the DNS can result in good and bad outcomes.

> By 2025, one third of all data will be processed real time. **When Industrial Internet of Things systems are scaled, data growth rates will be beyond exponential.**

Unfortunately, cyber crooks target vulnerable users after disasters, and this pandemic is a honey pot for them. With millions of people working at home, many for the first time, users are not always savvy with remote security protocols such as VPNs. Remote login credentials are an easy target. A DNS based hack of home and small office routers has stolen millions of passwords and cryptocurrency credentials, mainly in Europe and the USA. It achieved this by re-directing DNS queries to malicious addresses, offering services such as daily links to COVID-19 news,
and invaded domains through this.

Most recently, Nation states stand accused of attempting to hack COVID-19 research databases, in order to corrupt and to steal the most valuable of datasets that could lead to a vaccine.

NTT's Global Threat Intelligence Report 2020 points to high levels of innovation of cyber criminals and their ability to find the achilles heel of organisations. Over the past year, there has been a sharp rise in content management system attacks, because unstructured data is often th least protected and governed. The weaponisation of IoT is also on the rise, due to the immaturity of these architectures and the sheer volume of attack vectors that edge connections afford. Cyber reslience is an holistic capability encompassing sound technology and business practices and savvy monitoring of the continuously changing threat landscape.

Maturity – Ethics, Governance and Trust

The single greatest potential limitation of the internet is the eroding trust people place in it. Trust has taken a severe battering over the past 5 years, as people have wisenned up to non-consensual data misappropriation & monetisation, fake news, online exploitation, cyber crime and state based privacy intrusions. In the Digital World, each of the five tenets of the (abbreviated) Universal Declaration of Human Rights is frequently breached, giving rise to the movement to create a Universal Declaration of Digital Rights.

Singaporeans, who are generally compliant citizens, were asked by their government to share data that would assist with contract tracing, via a new app called TraceTogether. The adoption rate was only 20%. The Australian government is asking it's citizens to sign on to their government's iteration of TraceTogether, called COVIDSafe, aiming for 40% adoption. The consensus is that adoption is likely to be less than enough to make the application effective unless the government legislates around privacy protections. This is a lamentable example of the crisis of trust in the internet today.

Indeed, the father of the world wide web, Sir Tim Berners-Lee, is particularly unhappy with what's happened to the internet, specifically, the way that companies have come to own and control personal data. He's working with Massachusetts Institute of Technology, MIT, on a project that re-defines the concept of the internet as a whole. It's characterised by the decoupling of personal data and applications. This would distribute the control of data to individual entities. Called SOLID (social linked data), it aims to radically change how web apps work, improving privacy and enabling each of us to own our data and share it as we see fit.

The proposed set of conventions and tools build modular, decentralised social apps that don't perpetuate siloes of data, but can re-use existing data created from other apps. Essentially, we are decoupling our digital selves (our data) from the apps we use, which is a 180 degree design flip on the existing models of digital platforms and a major threat to their business models. This distributed web paradigm will ensure we can build out our digital twin coherently, according to our values, goals and needs.

> COVID-19 has disrupted the world, societies and economies will come out of this forever different. **The new normal will depend on the internet even moreso, it's now part of our atmosphere.**

Final Words

It's rare that we can use the term paradigm change legitimately. We can in this case. COVID-19 has disrupted the world, societies and economies will come out of this forever different. The new normal will depend on the internet even moreso, it's now part of our atmosphere. But it's reaching end of life in it's current form. Under a paradigm shift, it will literally run at the speed of light and with codified global security standards. And we have to believe that our data will flow at our behest, for our benefit, democratising this vital global infrastructure.

NTT

Together we do great things