Balancing Centralization and Decentralization in the network

The digital transition is a paradigm shift. It calls for regional sovereignty as Internet of Things needs huge ecosystems to be relevant to industry, security and good services for the people.

Co-creation with all actors in the ecosystem is of paramount importance.

We envisage solutions like a federated framework of millions of people who organize their SSI, Self-Sovereign Identity assisted by a large variety of custodians harnessed in a secure architecture from the chip up in a wide variety of wearables and phones that follow guidelines hardcoding social, cultural and a wide range of democratic value methodologies.

The cloud becomes the edge as we do AI and Machine Learning on the devices themselves.

This push-pull combination makes it very strong, unstoppable, fast and extremely disruptive.

The Internet of Things (Kranenburg, 2017) is a combination of a technological **push** - an ecology of barcodes, qr codes, rfid, active sensors, ipv6 - and a human **pull** for more and ever-growing connectivity with anything happening in the immediate and further out environment, a logical extension of the computing power in a single machine to the environment; the *environment as interface* (ubicomp, pervasive computing, and Mark Weiser's text The Computer for the 21th Century 1991).

This push-pull combination makes it very strong, unstoppable, fast and extremely disruptive.

In reality leadership is to address stress.

In this short talk I want to sketch three domains of research in a coordinated scope addressing anxiety and stress (whether in people or systems) in a structural way in the paradigm shift towards a ‘talkative planet’, ‘ambient intelligence’, cyber-physical systems, in short: a world in which every object is connected in an intranet or in an internet enabled Cloud or to currently emerging 5G networks.

The first domain lies in what is currently called pathology.

The first domain lies in the ability to make changes at system level and create building blocks that are so far out of the 'ordinary', that as they foreshadow a potential *next normal,* they cannot be immediately or ever implemented.

The structural element in the situation that has changed with the internet, web and internet of things is that the formative years of humans *have become data-driven* (constant input) they lack *the inner ability to reason with themselves.*

This ability – to create new foundations – has now been outsourced/taken over by *scripted serendipity* in the analytics of the content dashboards that inform current decision-making.

It is therefore vital that people are offered impulse free education.

The second domain lies in what is currently called reality..

The second domain lies in what is currently called reality.

Internet of Things/Ambient Intelligence is successful in so far as it **‘disappears into the fabric of everyday life’(**Weiser, 1999).

Digital Twins (the data body of any person, object, template) are not only separately collected and stored but are able to – in a very mundane way- act in real time in and on the ‘analogue’ object in the way that for example virtual implied car (taking into account information in the area, weather, surrounding cars...) can take over what was once the ‘real car’.

We are thus fully in Freud’s *Unheimliche*, growing up in a world in which it is no longer possible to differentiate between the real or fake.

This distributing of insecurity becomes the default.

The third domain lies in what is currently called the political

The third domain lies in what is currently called the political.

If efficiency is the only indicator, life becomes a very short meaning-less (pure procedural) loop.

Currently this pattern is scaled to the level of an entire society (fake news, Q, alternative facts…)

Concretely we must distribute security at two particular points, at **device level**(Kranenburg & Kavassalis, 2021) and the moment it enters into operation and at the **governance level** of society itself.

These three actualizations have a similar shattering effect on all levels: ontological (false/true), real (analogue/virtual) and idiolect (the impossibility to connect to an ‘I’ in order to grow, heal, become ‘whole’).

So we need a full practical philosophy for how to live ethically in a world of machines.

This philosophy should be able to produce hope, faith and forward looking resilience.

Secure at Device Level:

We need to give any device in an IoT ecosystem a unique identity.

We need to give any device in an IoT ecosystem a unique identity. This is a necessary step to create a layer of IoT security and control the risks, especially those associated with IoT deployment in home area networks and in public infrastructures. Such an identity can make these devices identifiable when they come online and improve the security of the use of the IoT devices within service chains, thus improving both cybersecurity and end-user's privacy. **These identities do not need to be persistent, but on the contrary, must be designed as ephemeral or disposable to avoid systematic tracking of the device and of the owners of the device, but they should become regulated, accepted and widely used.** They will obviously be based on the use of standardized digital certificates that will ensure proper authentication, transparency and authorization efficiency, and encryption.

Security at governance level: Analysis from 2012: Intel experts: *a total breakdown of society triggered by the failure of existing institutions to manage the Digital Transformation.*

In 2012 I was invited to talk about Internet of Things at an invitation-only event, run by the GFF and the Italian "Intelligence community", taking place in Rome that September. The session was entitled "Transformational Technologies #4: Implications for an Expanding Threat Environment". In the afternoon, participants - an impressive mix of senior intelligence, police and military experts broke out in five groups, each tasked with identifying major threats with their unfolding scenarios spanning the coming decade. The groups came back with different scenarios with five topping the list: one was focused on a military conflict, two were about biological disasters produced by DIY Bio. The revelation came with the focus of the remaining two*: a total breakdown of society triggered by the failure of existing institutions to manage the Digital Transformation.*

That is why a A 21th model builds Hot Spots and Cold Spots.

- van Kranenburg R. et al. (2020) Future Urban Smartness: Connectivity Zones with Disposable Identities. In: Augusto J.C. (eds) Handbook of Smart Cities. Springer, Cham. https://doi.org/10.1007/978-3-030-15145-4_56-1

Cold Spots why?

Digitalization” eroded the trust in symbolic institutions. Building resilience and **non digital futures.**

“Digitalization” eroded the trust in symbolic institutions through the subtle mean of dematerialization of money and the crude one of wealth dispossession, enabling that neo-feudal future some already predict. One after the other, digitalization cannibalised the public mission of core governance institutions, first through their internal operations then as vectors of transmission, evangelizing for the cause of a cyber-physical system encompassing all life on earth through legislation and budgets. In just about all societal dimensions, from military to health, education or agriculture, **the purposeless pursuit of digital efficiency** finds concrete manifestations in projects aiming to predict, control and manage human exchanges as if mechanical systems.” (Gaëlle Le Gars)

Hot Spots why? Because the current 5G deployments must have **a strong societal purpose and be integrated** : AI, VR, AR, in new crypto payment and token infrastructures that are in public hands.

- "..combination of 5G and wearables could make the smartphone revolution seem like a miniscule advancement. The latency of about 1 millisecond coupled with the high reliability of the network will enable a very high degree of real-time control – and this instantaneous and on-the-go attribute is what makes the content experience for – wearables so user-impressive (RIQ News 2020).
- Future 5G antennas for wearable application will be "compact, low-pro"le, comfortable and feature mechanical robustness, insensitivity to changes in user movements and robustness to deformations, varying mounting locations and body morphologies" (Aun et al. 2017).
- This means that information on the device can be stored throughout its lifetime (edge) and shared at specific moments with dedicated clouds to complete the security of the system which would operate in a closed-loop.

To conclude

Engineers, poets, philosophers and psychologists are needed in a new team.

@robvank

council