2.2.4. Trust, security, stability

We all want a secure and stable Internet that will inspire trust and confidence among users. The borderless nature of the Internet, the new economy, the IoT-driven cyber-physical asymmetric interdependency, the impact of the Internet on democracy and elections, finally its role in global crises – all this makes for a complex policy, legal and operational context for cybersecurity.

Almost all sectors use ICTs and rely on the Internet for everything from the simplest to the most strategic tasks. Global supply chains are increasingly interconnected, with their ICT systems and devices exposed to various cyber risks, such as online gender-based violence, cyberbullying, and misinformation. Neither the public nor the private sector can combat these borderless threats on their own. The technical community and civil society are key partners. As stakeholders seek to find ways to address cybersecurity concerns, collaboration is required in order to build awareness of vulnerabilities and incidents and to increase resilience against these complex, borderless cyber threats. To be sure, we will work towards a broad and overarching statement, expressing a common understanding of digital trust and security in the cyber sphere.

3. Challenges for the global digital dialogue

While the very notions of 'digital foreign policy' and 'Internet governance' have been around for a while, a lot remains to be done. To begin with, digital diplomacy falls behind the speeding technological revolution. It is challenging because it requires a greater coordination effort, which is difficult to obtain in a multistakeholder environment, but otherwise, it is a natural course of things and not a reason to worry. Instead, what really bothers me is that digital issues do not seem to be receiving as much attention as they deserve at a country level.

The impact of technologies is indisputable. Every country should have a clearly defined digital roadmap and an established advocacy scheme to pursue its digital priorities and influence global tendencies. Yet, the issue features surprisingly low on countries' diplomatic agendas, and that despite a growing consciousness of its importance. Digital issues are dealt with superficially or downright missing from the strategic diplomatic documents. Likewise, digital sherpas are conspicuous by their absence in diplomatic service. It is my firm belief that it must change. Digital diplomacy should be brought into focus, become mainstreamed and relevant at the highest political level. It is indispensable if we want to have a meaningful and consequential dialogue that translates into concrete actions rather than bog down in rhetoric.

3.1. What and how to regulate in the world of technology?

First of all, we need to discuss regulatory issues relating to financing, partnerships and digital market business models. This involves:

- Developing the capacity of regulators and service providers to build universal Internet access;
- Ensuring affordable Internet access while incentivising the existence and extent of local language content and locally relevant content;
- Creating a friendly environment for smaller-scale providers, including broadband cooperatives, municipal networks and local businesses by putting in place practices such as facilitating licence exemption and tax incentive schemes;
- Leveraging universal service and access funds (USAFs), which are financed primarily through contributions made by mobile network operators, to expand communications services to underserved areas and populations;
- Setting universal affordability targets with respect to digital connectivity: it would be far easier to develop a financing platform to close the global connectivity gap, including vulnerable and marginalised groups, had affordability been defined as, for example, 1 GB of mobile broadband data costing a certain tiny percentage (1,2,3…) of an average monthly household income.

Another major challenge is settling the rules governing the circulation of Big Data, a precondition for unlocking its vast economic potential. Why is it so important?

The Internet-driven solutions are generating vast amounts of non-personal data, raising questions of who owns it and how it should be used. Governments need to strike the right balance, i.e. to address privacy concerns without stifling beneficial innovations. This is all the more important that, in a digital age we live in, data has earned the status of commodity, underlying the creation of value and the satisfaction of human needs. It is derived from human activity, from observation of the natural environment phenomena (e.g. geodetic, meteorological data) and industrial processes (e.g. production line sensors). Data can be seen as a factor of production, along with capital and labour, an essential substrate of social and economic undertakings. Scientific research suggests that data-based activities have a paramount effect on growth nurturing compared to other factors. Investing in the data-driven economy is perhaps the most promising growth scenario for the post-pandemic era.

Raw non-personal data should circulate in the economy, leading to welfare proliferation. This requires the resolve and effort pooling from governments to facilitate the forming of robust and liquid data markets. Currently, the landscape is dominated by isolated data collection systems dominate that create inaccessible silos. For data potential to be fully tapped, standards must be set for its circulation. Otherwise, businesses will remain reluctant to share, exchange or sell it.

Likewise, the time has come for the provisions on the free flow of raw non-personal data to be included in international free trade agreements. For this to happen, we need to work together within the UN, OECD, and WTO to overcome regulatory hurdles and reach a viable and operational consensus.

Inevitably, where there is data, there are data breaches, since with more people being brought online, vulnerabilities arise. The cost of data breaches is expected to grow annually at 11 per cent, from $3 trillion in 2019 to over $5 trillion in 2024.[7] As the nature of cyber-attacks evolve, cybersecurity needs to adapt accordingly. System developers must invent safer devices. Operators must leverage AI to develop new security techniques to protect networks and platforms against scammers and attackers. Services must be designed to run with the minimum of user information. And governments must work in concert towards commonly accepted measures – ones that will protect the cyber sphere without disrupting it.

Should the Internet become overregulated, it will lose its innate appeal. It is obvious that governments should protect their citizens, but this must be done in a collaborative way, with all stakeholders involved. If controls are imposed too tightly or/and in an erratic manner, they will do more harm than good. The Internet is a dynamic organism that functions like a system of interconnected vessels. No single actor can make a positive difference to its workings alone. Unilateral moves, attempting to draw sovereign lines and rules are ineffective, counterproductive and ultimately doomed to failure.

[7] *The Future of Cybercrime & Security: Threat Analysis, Impact Assessment & Mitigation Strategies 2019-2024* (Jupiter Research, August 2019).

3.2. What and how to finance in the world of technologies?

Securing sustainable Internet connectivity requires substantial spending. The task is twice as challenging in developing countries. For instance, the ITU/UNESCO Broadband Commission for Sustainable Development estimates that achieving universal, affordable and quality Internet access by 2030 across Africa may cost as much as $100 billion.[8]

The characteristic feature of the ICT infrastructure is that most of its financing has traditionally come from private-sector companies who make substantial outlays seeking commercial return. Governments, sovereign funds and multilateral players, such as development banks, have played a relatively minor role, especially compared to the scale of their investment in other infrastructure sectors. The reason for this is a tendency to view Internet provision as a strictly private-sector activity rather than a public right. In the United States, for example, the public sector's share of ICT infrastructure investments is nearly zero, while the share of public investment in transportation and water and sewage infrastructure is about 90 per cent.[9] Moreover, procurement requirements of public institutions, which can add months or even years to project timelines, are at odds with the rapid speed of progress among ICT technologies and, therefore, undermine the suitability of public investment processes for ICT infrastructure projects.

Interestingly, equity markets, which eagerly get involved in various infrastructure projects, are absent from the ICT sector, dominated by industry players (network operators, ISPs, tower builders, satellite companies). Many private-sector investors exclude ICT infrastructure assets from their portfolios altogether, considering them too complex and largely the domain of network operators and ISPs. And those who do make infrastructure investments avoid going beyond core population centres. Indeed, the cost of extending infrastructure to remote or sparsely populated areas is unprofitable to mobile network operators unless they receive significant support from public-sector or international funds.

Meeting the global need for advanced network infrastructure requires the development of financing models that account for returns on investment beyond simple business cases. In most developed and emerging markets, the public sector must improve the attractiveness of ICT investments.

[8] *Connecting Africa Through Broadband: A Strategy for Doubling Connectivity by 2021 and Reaching Universal Access by 2030* (Broadband Commission for Sustainable Development, ITU and UNESCO, Geneva, 2019).

[9] *Bridging Global Infrastructure Gaps* (McKinsey Global Institute, June 2016).

This can be done through blended financing and risk-sharing arrangements: government subsidies and operator fees would be pooled over time to pay for infrastructure expansion in areas that are sparsely populated, topologically challenging or difficult to serve. These arrangements help investors overcome many barriers, such as low returns relative to risk or inefficient local markets. Universal service and access funds (USAFs), set up by governments to address gaps in coverage that cannot be served by the private sector alone, have a prominent role to play here.

Infrastructure projects can be bundled into dedicated investment vehicles or funds that reduce exposure to individual risks of geography or technology and enable smaller projects to attract capital from larger investors. However, their use in ICT is limited. For example, only 3 per cent of all deals undertaken by infrastructure funds in Asia from 2010 through 2015 involved telecommunications, compared with 44 per cent involving energy, 22 per cent utilities and 16 per cent transportation.[10] Another option allowing for risk mitigation is bond issue by international finance institutions who then invest in eligible projects through financial intermediaries.

3.3. Technologies and sustainable development

On one hand, technological progress inevitably with pollution (from infrastructure exploitation and manufacturing/disposal of electronic devices) and power consumption. ICT operations are estimated to represent up to 20 per cent of global electricity demand, with one third stemming from data centres alone.[11] On the other hand, the Internet-driven Fourth Industrial Revolution has largely succeeded in decoupling economic growth and environmental damage. ICTs have steered the economy away from energy and material-intensive activities, ushering in three major phenomena: dematerialisation (less resource input), virtualisation (substitution of tangible goods), and demobilisation (substitution of travel).

Not only less harm is caused to the planet, but actually a lot of good is done to protect it (electronic monitoring, remote sensing etc.). The environmental SDGs cannot be met without frontier technologies and inte-

[10] Georg Inderst, *Infrastructure Investment, Private Finance, and Institutional Investors: Asia from a Global Perspective* (2016) 555 Asian Development Bank Institute, Working Paper Series.

[11] Nicola Jones, 'How to stop data centers from gobbling up the world's electricity' (2018) 561 7722.