UNITED NATIONS COMMISSION ON SCIENCE AND TECHNOLOGY FOR DEVELOPMENT (CSTD), twenty-fourth session
Geneva, 17-21 May 2021

Progress made in the implementation of and follow-up to the outcomes of the World Summit on the Information Society at the regional and international level

Statement submitted by

Mr. Vinton G. Cerf
Vice President and Chief Internet Evangelist for Google

DISCLAIMER: The views presented here are the contributors' and do not necessarily reflect the views and position of the United Nations or the United Nations Conference on Trade and Development.

On WSIS Goals Progress

Vinton G. Cerf
VP, Google

FINAL
5/19/2021 0745 ET

By any reasonable metric, substantial progress has been made on a number of WSIS goals since 2005. Most visibly, the arrival of the smartphone in 2007 and the rapid growth of 4G mobile networks has provided Internet and World Wide Web access to literally billions. In addition, there has been very notable growth in subsea optical fiber networks linking the continents in a web of glass. In this same time period, significant MEO and now LEO satellite capability is either operational or on the horizon. In the latter case, especially, there are multiple potential and existing providers. Literally millions of smartphone applications have been developed and downloaded into billions of mobile phones. We can also cite progress in electronic funds transfer capabilities, even without taking into account so-called cryptocurrencies that remain somewhat problematic in terms of stability. Mobile and laptop or pad payment apps are widely used. In some parts of the world, paper or coin currency has been largely supplanted with electronic analogs.

In this same time period, we have seen the creation and spread of a number of so-called social media. Some have thrived and some have come and gone but these are widely popular. Streaming media for audio and video are very popular where Internet access has adequate capacity. Content Distribution Networks reduce the cross-Internet traffic load and reduce latency by distributing content to servers close to their users. During the past 15 months of the global COVID-19 pandemic, heavier than ever use of the Internet has emerged in support of remote work, education and healthcare, especially interactive video-conferencing.

The so-called “Internet of Things” is a rapidly growing business with devices and online services to support them emerging persistently. The utility of these devices is increasingly apparent but their vulnerabilities add incentives to improve security and attention to securely updating software to eliminate exploitation.

In this same period, however, we have discovered that the reduced barriers to access to online services has downside risks. Increased dependence on online products and services means that when they are inaccessible or fail to operate, there are cascading and potentially negative side effects. Malware is widespread as are so-called “phishing” attacks, denial-of-service attacks and the propagation of misinformation and disinformation with consequent potential social and economic harms. These concerns have heightened interest in protecting users through training, technology and law enforcement actions and raise important questions about and interest in cooperation across national boundaries. The Digital Cooperation initiatives launched by Secretary-General of the UN, Antonio Guterres has given considerable impetus to cross-border collaboration.

At the same time, concern for citizen safety has driven some national authorities to seek to limit transborder data flow under the rubric of “data sovereignty.” While often well-intended, such measures can have significant negative side-effects for the resilience of cloud computing services and resistance to data loss, harming public, private and civil society interests. There is little doubt in my mind, however, that more cooperation among governments and private sector entities will be needed to protect citizen interests. Improved tools for safety, security and privacy as well as strong authentication and use of public key cryptography will be needed by all sectors making use of the Internet on a regular basis.

A popular development in digital technology is the concept of open source. A number of open source libraries have been created, some of them operating at very large, international scale. They have allowed rapid development of new applications by saving developers the trouble of inventing new operating systems and offering them pre-fabricated building blocks out of which to develop myriad new applications. There are millions of applications in the mobile “app-stores” from which to choose. This concept, while enormously enabling, is also a source of serious potential vulnerability. Just because the source code is available for scrutiny does not mean that all its “bugs” have been discovered. Indeed, many of the vulnerabilities exploited by bad actors arise from the use of inadequately examined source code. This suggests that the “bug bounty” business may be a thriving concern at least in this decade and likely for some time to come. Developers really need new program development environments that will expose exploitable mistakes before the software is put to use in the field.

Another popular tool for user protection is found in “two factor authentication” by which means a physical device containing cryptographic information only accessible to the user is employed to augment or even replace the more familiar but vulnerable username and password practice of the past and present. A mobile phone, properly equipped, can become a “second factor” augmenting or replacing the older methods of identification. A separate security device could also be used and could contain cryptographic information for hundreds of distinct accounts. An important consideration will be standardization of such methods so as to give them legal standing when questions of due diligence and reasonable security protections are at issue in legal settings.

The remaining years of the 2020s will provide serious opportunities to improve the safety, security, privacy, sustainability and reliability of digital technologies, allowing us to harvest their beneficial power while limiting their potential hazards.