What future governance now that we know ?

Internet Governance (IG) has been the topic of endless discussions since WSIS onset in 2001. A majority of States insist in having equal weight in decisions bearing not just on technical matters, but on public policies, economic and societal impacts as well, at national and international level. However, the US government (USG) has not in any way lowered its determination to pursue its spying and mass surveillance operations, and keep unilateral control over internet through a private californian company (ICANN) created in 1998 for this specific purpose.

Rhetorics and wishful scenarios may go on for any number of years, without predictable outcome. While ideas and viewpoints may gradually become more flexible and negotiable, over time the dominant party keeps expanding its power to the point of being so entrenched as to make negotiation irrelevant. Discussions without capacity for counteractions is a losing game. Are citizens of all countries to remain sitting ducks waiting to be digitized and monetized ? An ultimate goal of the cyber-colonisation.

What actions are possible ?

Unless it works for USG's interest, any action requiring USG's agreement will be blocked. This is routine realpolitik. Hence, possible actions are those which can be implemented without USG's agreement, e.g.:

- apply national/regional laws on personal data privacy,
- apply national/regional fiscal laws to tax evaders,
- impose penalties on abusive market dominance,
- exclude illegitimate monopolies from major contracts,
- balance investment/revenues between operators, content providers, ISPs and media,
- protect natural plants from illegitimate patents,
- create national/regional domain registries independent from ICANN,
- open competition between multiple DNS roots,
- use open source software,

- promote user friendly end-to-end email encryption,
- keep object identifiers registries and standards under trade control (ISO),
- boost research/development on future internet (RINA).
- . . more ?

Some readers may think of a laundry list. In the context of standing up a hyperpower a first level of defense is to make spying and predatory operations more costly. A second level is to chip away enough parcels of independence to acquire some bargaining potential. On a longer term the objective is to make countries more resistant and better prepared to aggressive intrusions.

A good number of suggested actions need no more detail, as they are self-explanatory. Let's develop those which may not be.

- **protect natural plants from illegitimate patents.**

Example: an insect resistant indigenous pepper variety grows in some less developed country (LDC). A multinational chemical group adds some useless ingredient to the seeds, and takes a patent. Thereafter it sues local farmers for growing alleged patented pepper without a licence.

- **create national/regional domain registries independent from ICANN.**

Top Level Domains (TLD) like .com, .net, .org, are familiar even to non internet users. Country code TLD (ccTLD) like .cn, .de, .fr, it, .us are also well known, others like .bz, .gl, .tp, .vi are much less known.

New TLDs being presently introduced like .bike, .construction, .guru, .photography, .singles, are largely unknown.

The USG imposed ICANN (created in 1998) as a monopoly in charge of all (cc)TLD registrations. This unilateral decision has no legitimate international basis. A good reason for such an anticompetitive status was to endow ICANN with a permanent cash cow fed with domain rental fees paid by internet users.

As usual with monopolies, and in this case backed by the USG, ICANN's top priority is making more money for its lavish life style and buying friends. Being in the position of TLD regulator and financial beneficiary is a blatant case of conflictual interests.

There is a dire need for cleaning up the ICANN house and place it in competition with other actors taking care of users interests.

Actually since 1996, before ICANN was created, independent registries have sprung up, and operated during a number of years, or still exist, e.g. Name-Space, Cesidianroot-Europe, OpenNic, Slash/dot, Name.coin, etc. An undetermined population of private registries operate out of conventional institutions and remain mostly invisible. Whether due to ignorance, misinformation, or ICANN monopoly, independent registries are presently limited to niche markets. As no international legal instrument protects the ICANN monopoly the market could swing to other directions should States or large institutions change policy, or lack thereof.

- **open competition between multiple DNS roots,**

In the domain name field the term "root" designates a file containing a collection of TLD parameters. This file is duplicated within "name servers" queried by browsers or other applications for getting an IP address associated with a TLD. In a nutshell this is the replica of looking up a subscriber's number in a phone directory.

Root is a technical concept, a container of TLD parameters. **Registry** is an organization managing domain users and their identifiers. A registry may use its own root (OpenNic), or the root of another organization (PIR, Public Internet Registry for .org uses the ICANN's root).

An ICANN dogma is the need for a unique global (i.e. USG controlled) root. As mentioned earlier independent registries and multiple roots have been in operation for longer than ICANN's life, but they don't fit well in a monopolist empire. Curiously Google and OpenDNS, which are not registries, use their own roots, which are ICANN's copies.

A further analysis of a multiple roots environment is worth a longer development in another article.

- **promote user friendly end-to-end email encryption.**

After Edward Snowden's publications it is no longer possible to handle security with benign neglect. Many, but not all, organizations will try harder to integrate security in their procedures. This will be reinforced by the commercial pressure of the security industry. Encryption is the basic ingredient of secure communications; it is used routinely in closed environments, but practically nowhere in open environments. Email is by and large the dominant service for private and professional exchanges. As long as encryption is clumsy or takes more time it will not catch up in public use. In addition there should be a limited set of standardized protocols implemented in all mailers. At this point campaigns inciting users to adopt security could have a chance to succeed.

- **keep object identifiers registries and standards under trade control (ISO).**

It is already projected that the order of magnitude of objects in the internet will be 3 to 5 times larger than the number of humans. Tools will be necessary for registration, retrieval, and exchange of identifiers. Applying DNS tools for handling this type of data seems inadequate and unrealistic. An example of such practical system is GS1 for bar codes and RFID. It is successful because it is carefully tailored to the needs of a specific trade: worldwide distribution of mass produced consumer goods typically available in supermarkets. Automobile, chemicals, hospitals, wine, would have different needs. If the identifier management market falls in the hands of a world monopoly, it will impose its own proprietary standards irrespective of specific trade needs, and distort manufacturing or distribution processes for its own profit.

Care should be taken to foster consensus within trades for identifier management standards anchored in a reputable international organisation such as ISO.

- **boost research/development on future internet (RINA).**

As it stands today internet is an overpatched experimental system based on 40-year old concepts. The writing on the wall is "obsolescence". Research on future internet has been reintroduced in the past ten years, mainly as separate projects without focusing on a specific operational target. Somehow a team at Boston U came up with a breakthrough in network design: "Patterns in Network Architecture" by John Day. The system name is RINA, recursive internetwork architecture. European teams got contracts from the EU Commission research programme to expand the initial platform in developing applications. This is an opportunity for a new generation of designers to close the security gaps of the legacy internet.

- **trust is gone.**

This is matter of fact, even though trust is subjective. "If you want peace, prepare war" is an old mantra. We don't really know how the US people will adjust to mass surveillance, which for decades was supposed to exist only in countries like China, Russia, East Germany, and many others. The logistics has reached a point from which there may be no return. A totalitarian regime more orwellian than ever might take over. We have to convince our goverments and fellow citizens to steer away from that model, and technology. We don't want to live in this kind of society, do we ?

Louis Pouzin@eurolinc.eu
v0.1 February 2014