NRIs Collaborative Session: Digital competences to harness technologies for sustainable development – Cases and Approaches

Carlos A. Afonso

22-12-2017

Digital technologies have reached new heights in their complexity, including the diversity and complexity of networked systems and applications.

As we speak, cryptocurrency miners may have installed a script on your mobile or desktop browser that, whenever your device is connected to the network, it helps mine cryptocurrencies to a stranger. As we speak, news comes from a country in which a bank has depleted the stock of high-performance video cards in the market – to use in cryptocurrency mining.

As we speak, algorithms are used to decide hiring and firing, releasing or holding people in prison, approving or refusing credit (or offering credit under conditions that vary according to the profile analyzed by the algorithm). Data from a group of researchers point to the possibility that in the next 10 to 20 years about half of today's jobs in developed countries will be threatened by algorithms, and 40 percent of the top 500 companies may disappear within a decade.

They estimate that between 2020 and 2060 supercomputers will exceed human skills in almost every area. People of the caliber of Elon Musk, Bill Gates and Steve Wozniak warn that this mechatronic "super-intelligence" network is a serious threat to humanity, possibly even more dangerous than nuclear weapons.

And as we speak, IoT, one of the new fashionable talk topics, is already present in our homes and pockets for a long time, and hundreds of millions of devices have been deployed without proper security protections. In most cases, no one knows who actually built the device, or who is responsible for the firmware running in it -- no question that there will never be a firmware update. Right now, major ransomware incidents are happening using IoT devices as means of attack.

How do these results and deployments impact in real life, are they to be automatically accepted by decision-makers as valid or true? Some analysts have provided abundant functioning examples of the dangers of trusting human decision-making to algorithms. Mathematician Cathy O'Neil is an outstanding example of a researcher pointing precisely to these dangers in several typical applications of these systems.

Today, social networking or transaction algorithms know more about us than our family or ourselves. And they can even offer recommendations for decisions that look good, even if they are not our decisions. A situation where we are increasingly remotely controlled – the more these systems know about us, the more our actions can be predetermined by others. It's something like going from computer programming to people programming.

It's the algorithms of mass destruction, or weapons of *math* destruction, in Cathy O'Neil's precise expression.[1]

What should concern us even more (as if we needed to be more frightened) is that this

---

[1] Cathy O'Neil. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown Publishers, 2016. 272p.

whole techno-entangled apparatus is not the privilege of the super-rich manipulating governments, or state systems of monitoring and fighting crime, but it is also within the reach of common hackers who invade and extract the data they want from the Pentagon, the White House, Equifax, the NSA, or take a whole network for ransom (as in the case of England's NHS captured by ransomware), and if you know that these vulnerabilities happen in the US, what to expect in other countries?

We are at a crossroads. If ever more powerful algorithms are controlled by a narrow group of decision makers, reducing our self-determination or the balancing opinion of human common sense, researchers say, we will fall back on what they call a sort of feudalism 2.0.

And here I reach a topic I would like to have considered for this session: the challenge of preparing public service, public servants, the public sector, political decision-makers to better understand what is going on. We see in the many targets described for the 17 SGDs that the 15 ones mentioning or related to capacity development seem to avoid this specific issue of formation of the public sector. On several fronts, we learn of new bills of law (dozens of them) trying to regulate, modify, repress instances of technology for which the proposers have no idea of what they are talking about.

We have seen a glaring example of this in the debate on net neutrality in the USA right now. We see many examples of bills proposing blockades, censorship, content control etc which usually involve complete lack of knowledge of the functionings of networked systems. And as a result politicians may be manipulated by powerful economic interests to insert biased laws favoring their businesses. How to create capacity development mechanisms which will lead to better law-making and more informed decision-making by the public sector (a problem for any field, but particularly acute when it involves the complexities of the networked systems of today and tomorrow)?