A Perfect World? Risks and Threats in the Information Society

Gustavo A. Masera★
& Javier Ulises Ortiz★★

About the Authors

★Gustavo A. Masera, Ph.D. in History, National University of Córdoba. Multidisciplinary Institute of Contemporary Social Studies (IMESC-IDEHESI), Faculty of Philosophy and Letters, National University of Cuyo, (Mendoza), Argentina. Email for correspondence: gustavo.masera@gmail.com
★★ Javier Ulises Ortiz, Ph.D. in Political Science, Universidad del Salvador. Professor and research at National Defense University, (Buenos Aires), Argentina. Email for correspondence: juo425@yahoo.com.ar

ABSTRACT

The document provides an approximation to the issue of global systemic risks in the information society and, in particular, those having an impact on critical infrastructures. In order to do this, the experience of mature developed countries is taken into account from the perspective of agencies and authors specialized in these issues. The discussion will allow not only for the comprehension of the risks associated to the development of these infrastructures but also value governance as a participative mechanism for risk management. The result of this work will have useful features as support for decision making and the formulation of domestic and foreign public policies, and especially support the debate being born in Latin America.

Keyword: Risks, Critical Infrastructures, Information society, Latin America

"New and terrifying events are happening as we take our first steps into the 21st Century", OECD, Emerging systemic risks in the 21st Century.

CITATION:
Gustavo A. Masera & Javier Ulises Ortiz (2018). "A Perfect world? Risks and Threats in the Information Society." *Inter. J. Res. Methodol. Soc. Sci.*, Vol., 4, No. 1: pp. 36-49. (Jan. – Mar. 2018); ISSN: 2415-0371.

1.0 THE INFORMATION SOCIETY

The shared conception in the academic world is that scientific-technological changes which have taken place over the last decades of the 20th Century constitute a theoretical-conceptual challenge, an opportunity field for economic evolution and a set of threats and risks for society as a system (Bischoff, 2008).

The discussion posited in the work will allow to: (i) To sustain the elaboration of appropriate strategies for the insertion of Latin America in the international community known as "information society" (IS), in a more theoretical plane; (ii) To plan the path of growth of critical infrastructures bearing in mind the risks that goes with them; and (iii) To implement participation mechanisms for the management of the IS and of critical infrastructures based on sustainable development and governance (Bevir, 2007).

In a more operative plane, to formulate bases for public policies aimed at the management and regulation of risks. It is in this frame that an approximation is done to the issues of the information society. In particular, the risks of critical infrastructures are considered, taking into account the experiences of maturely industrialized countries, think-tanks perceptions and authors specialized in these matters (IRGC, 2006). A realistic analysis identifies the potentialities, limitations and dangers involved in the development of the IS. The biggest gain will possible be a comprehension of the entirety of positive and negative aspects and, above all, its implications for the IS.

The first thing to consider is that the international contemporary system has undergone enormous transformations over the last few decades, with many of these changes coming over the last few years. Amongst these transformations, we can identify:

The unification of the world economy through a multidimensional and complex process of globalization in an international setting which emphasizes existing asymmetries and cannot but lead to an unequal development of the different actors. In this new world we find that centrifuge forces of dispersion, fragmentation and crisis (with important geographical transference of industrial installations and introduction of technological changes) live together with centripetal forces of intertwining and interdependence between different regions of the world (having as principal vector the interconnection of the infrastructures of information, energy and transport). This process is accompanied by a growing internalization of diverse actors such as companies, financial institutions, etc. (Masera, 2010; Nye and Donahue, 2000).

The centrality of the socio-technological paradigm endlessly multiplies new models of scientific-technological production. These new models simultaneously affect the pre-existent means of production (from agriculture to traditional industries, such as the automobile sector) and give origin to new areas of products and services (for instance the production and distribution of alternative sources of energy). These new models are generally localized in systems of high specialization territorial innovation enhanced by digital infrastructures and communication networks of universal access (Mansell, 2009; Bernal-Meza and Masera, 2007).

A renewed tendency to the formation of regional spaces of commerce and investments with open agendas for the discussion of a variety of issues and the degree of depth for negotiations within a regionalization dynamics of political, economic and cultural systems. These integrated spaces tend to cut across national borders and jurisdictional spaces and are strengthened by infrastructure networks which facilitate contact and exchanges (Masera, 2010).

The emergence of systemic risks with global dimension fed by the same factors which make the abovementioned points possible: economic unification, technological intensity and regionalization. Some recent examples that can be cited are: the 2008/09 international financial crisis, economic recession, aviary and a flu pandemics, food crisis, the commercial negotiations of the World Trade Organization (WTO) getting stuck, problems with supply of gas from Russia to Europe, power blackouts of great dimensions in the US and Europe, consequences of climate change (Lippert, 2016), etc. These risks can affect the socio-political stability and the economic prosperity of many nations. In addition they can provoke other changes that can have lasting effects on the distribution of power among countries and regions, and even catastrophic impacts on the most vulnerable societies (Masera, 2008).

The global society of the beginning of the 21st Century is characterized by the massive use of technology information and of communications (ICT).This insertion of the ICT is changing the modes of governing, producing, socializing, and offer and access to goods and services. In

advanced industrial societies, this evolution has given place to the birth of the IS (Webster, 2006; 2002). Even if there is not universally accepted definition, it can be stated that the information society is a post-industrial society (or knowledge society) where the generation, circulation, manipulation and use of information processed through computers and digital communications is an essential component to social, political and economic activities (Hadkiewicz, W. and P. Gawowicz, 2013; Peres, Hilbert, 2009; Comisión Europea, 2003).

2.0 SYSTEMIC RISKS: GENERAL CONCEPTS

Talking about risks that can affect society as a whole, the issue of global emerging risks of a systemic nature cannot be ignored (IRGC, 2010).

The international setting has seen the emergence of some hot issues since the end of the 90s such as the evidence of climatic change and its effects on natural resources, accelerated population growth and migratory flows, the decay of public services in less developed regions and social tensions in societies which receive immigration. It has also been established that the technologies used to solve some of these problems (for instance, new vaccines or seeds) or to promote economic development (with ICT as a priority) are not risk-free. More importantly there is a maturity in the understanding (as it has been partially experienced) that these risks have the capacity to cause strong impacts on societies, with even the potential for destructuring them.

The 9/11 attacks in USA and other events like the massive blackout in big urban agglomerations, have demonstrated that the unlimited security in a complex world in impossible (Ortiz, 2008). The cyberspace is the new "Athena´s Camp" for the development of new conflicts, many of "asymmetrical" type (Thomas, 2005). In the developed countries the concepts of cyberwarfare, information warfare and information operations appear as new governmental cybersecurity / cyberdefense doctrines) (Castells, 2002).

According to the sociologist Manuel Castells the 9/11 was the beginning of the first world war of the XXI century, the "net war" that attempt to "impose their objectives by using the only efficient weapon in its technological and military inferiority situation."

In May, 2007 the Estonia computing system was attacked through Internet by a half of millions of computers. Estonia was paralyzed during some weeks y needed the NATO help. James Appathurai, a NATO spokesman, said in relation with the attack: "the XXI century is not of tanks and artillery" and after the meeting of the NATO chiefs of June 14th, 2007, he summarized that: "everybody agreed that it is indispensable to improve the protection capability of the computing systems of critical importance" (BBC, 2007).

As an answer to these attacks, a new concept in defense and security matters appears: the Protection of the Critical Information Infrastructure (PCII) to reach bigger possibilities of endurance against these attacks and accidents. It is necessary to identify and secure the CII to avoid a new "Mutual Assured Destruction" for this new age. The cooperation hemispheric agenda for the regional security and defense starts to incorporate these definitions so that the member countries develop their own concepts. The telecommunication (optic fiber, digitalization, computing) are the technologic infrastructure of the globalization that make possible the strategic decision making in real time at a global scale (Ortiz, 2008).

Since the late '90s the nations acquire new forms like the "Digital State" (Keyworth, 1998) or "Net-State" (Castells, 1998), and their sovereignties are enlarged. Whether by attack or by accident (blackout in megalopolis), the risks of not having prevision systems, early warnings and fast answer based on the emergency plans, can be devastating

This danger affects societies with advanced economies and those in process of development though with different characteristics. What is surely different is the faculty of resistance, resilience and elasticity shown in these three kinds of societies regarding risks. As a result, the fundamental issue for the governance of societies, specifically in Latin America, is that of institutions, decision-making processes and the instruments to face these inevitable risks. To participate in the 21st

Century world means to be exposed to the risks already mentioned and the biggest risk is to ignore this situation.

As examples, we can point out cases that allow us to hypothesize other possible crisis of a bigger, more dramatic dimension:

- "Mad cow" disease (especially in Europe and particularly in the U.K.) which involved costs, economic effects, changes in consumption and commerce patterns.

- The aviary flu, which had an effect on international tourism, on consumption of foods, on human health and even on education and scientific investigation programs.

- A strong conflict between new OGM products and traditional harvests (with advances in biology, genomic structures, etc.) This generates social acceptance effects, changes in genetic diversity, effects on world commerce and on the monopoly of patents.

A set of new applications and materials based on nanotechnology and its applications in food products and cosmetics which has effects on health, destruction of markets with seasonal changes of products and the strengthening of patents monopoly.

The possible faults in ICT systems used uniformly around the planet (e.g. operative systems, ofimatics programs), and the possibility of cyber-attacks on the whole of society, like in Estonia in 2007 and Georgia in 2008 (Ortiz, 2012; Saadawi. and Jordan 2011) and in the European Union in 2017.

The fragility of the security and safety systems in critical installations as in nuclear plants, with Chernobyl symbolically, showing the borders of modernity. The acceleration of changes and contagion mechanisms in an interdependent world economy imposed by the velocity, connectivity and intangibility in the different infrastructures but, especially in the financial one (IRGC, 2016).

We can add natural disasters to the list (like earthquakes and tsunamis) which have affected all civilizations in different historical epochs but, whose effects could be more disastrous nowadays due to the difficult continuity of life after the destruction of basic infrastructures as shown by the case of New Orleans after Hurricane Katrina in 2005 (Moynihan, 2009). There is also the case of disasters caused by human action on nature such as intentional fires. All this gives the impression that society is at moments on the edge of losing control when faced with important risks, threats, disasters and non-conventional crisis (IRGC, 2009).

Some of the questions that can be asked are:

Do we know the risks to which our societies are exposed?

Do we know the fragility of our society regarding these risks?

Are we prepared to face them? Do we know how to prevent, intervene and/or mitigate the consequences?

Do we know what capacities we have for countering them, be them organizational, technological or human? Have we planned what capacities we will have to develop over the next few years in order to be prepared for future risks? Who has to take which decisions? Which is the role of public authorities and which is the role of infrastructure operators? And, what are the voice and the role of civil society?

3.0 SYSTEMIC RISKS: DEBATE AND APPROACH

In a first approach, we privilege the identification of the forces generating systemic changes. These forces permit the formation of risks in 4 fundamental contexts: demography, environment, technology and socioeconomic structures. It cannot only be considered that new changes may arise but also, that the alteration of conditions may imply the spreading of negative consequences. This would imply the transformation of the channels through which "accidents" spread and might even alter the kind of social responses (OECD, 2003).

Of course, there are technical and non-technical dimensions to the problem of risks. The technical elements may, up to a point (in the absence of local availability), be acquired in the world market, taking as an example the best practices carried out in advanced countries. Technical elements though can neither be improvised nor copy from other experiences because they depend intrinsically on the risk environment and the society being affected; also, its appreciation depends on the psychological and societal experience of the risk. Besides, it depends on the perception of the possibility of it happening, the magnitude of its possible impacts and the importance of preventing negative situations which are by nature fortuitous and not predictable.

Let us remember that Thompson started by distinguishing (1990) between real risks (what may occur, with negative consequences that can happen with a statistically known probability, quakes, plane crashes), observed risks (what can be deducted from models or studies like the possible effects of an epidemics) and, perceived risks (subjective judgements in the absence of models or previous knowledge) like the effect of future nano-technological products. There are differences between risk and risk perception (Campbell, 2007).

It is possible to defend the following idea: Even if models and statistics may help, the perception of risk is always a persona/social judgement and it does not always coincides with outer reality. This is specially the case of complex systems like infrastructures. The point being that nobody really knows for sure how these will function in abnormal situations (at least the very significant ones like large integrated electrical systems, the Internet, etc.). There is not and there cannot be any certitude about the probability and the effects of risks on complex systems. The point about infrastructures is above all to understand their tendency to grow and develop. This is the prevailing direction: growing complexity (Pierre and Peters, 2005).

Therefore, the concept of risk is relative: the same effects can be rated in diverse manners by different societies and people. Moreover, there are risks that do not affect all citizens in the same way – and there can be winners and losers with different risks and options regarding action (Lechte, 2003).

So, we have to talk about the acceptability of risks, including the activities for preventing, monitoring, acting against and mitigating them.

In any case, assessment, management and evaluation of alternatives of risks is fundamental since there are critical systems whose failure may produce the collapse of society, just as it has happened before in the history of mankind.

Some factors that must be considered when talking about risks are:

- Uncertainty as regards the probability of occurrence, for instance, what is the probability of a catastrophic failure in an infrastructure in 10 years?
- Uncertainty about the severity of the impact of a catastrophic failure, for instance, causing a huge blackout (Gheorghe et al., 2005).
- Possible victims and damages (to health, environment, properties) and their knowledge about the existence of risks, dangers, etc.
- Whether it is possible to reverse negative effects.
- Compensation for being exposed to risk, or the existence of the option to choose not to be exposed.
- Benefits and dangers (and costs) for the different actors.

4.0 RISKS IN THE INFORMATION SOCIETY

Within the general realm of contemporary risks, it is necessary to consider the specific risks arising in the context of the IS.

The concept IS makes reference to a new paradigm whose orienting criteria show a new type of organization still being built (CEPAL, 2003). The IS, is the result of the action of technological systems enabled and empowered by the new information and communication technologies together with the progressive processes of digitalization. The fast planet-wide spreading of this expression has been given impulse by the action of various international organisms together with the publicity owed to some futurologists and enterprise management gurus (Masera, 2010).

As objective data about it coming into the scene, there are numerous initiatives like summit meetings, seminars, observatory bodies, publications, forums and entities which have taken place recently organized with the purpose of analysing the transition towards this digital society. An illustration of this took place in 2006 with May 17 being declared IS's world day by the UN. Arising from what was agreed upon in Tunisia 2005, "World Summit IS", resolution A/RES/60/252 of the General Assembly was approved with the objective of commemorating the 140th birthday of the International Telecommunication Union founded in 1865, which was the first worldwide intergovernmental organization (ITU, 2006).

Just over a decade ago, Ulrich Beck (1992) introduced and made popular the concept of "risk society". Beck points out problems and criticises the limitations of the current society but does not go as far as proposing a way of managing these problems. One may share his call for a participative democracy, but, the idea that the current technology has created new risks can be rescued as well as that of qualitatively different dangers, when compared to those of the past (Mythen, 2004).

It can be averred beyond doubt that no system is perfect. In the IS there exist risks, threats and vulnerabilities -and points close to errors, failures, security, etc- unbeknownst before. (Masera, 2010). The ICTs present solutions which appear dazzling for their effects of advanced modernity. Actually, its modernity resides both in knowing how to make use of its functionalities as well as knowing how to manage its limitations. On the other hand, as many of current technological risks do not respect national frontiers, there also arise problems relative to regional or international coordination policies regarding them.

The challenge is that the matter of weak points which appear when connecting the "whole" to Internet must be confronted rapidly, as they might affect the future of commerce, government, hospitals, banks, energy, etc. The so-called 'Information and Communication Technology' (ITC), which is the basic support for the IS, is the result of the interconnection of telephony systems to the Internet, and satellite communications. It can be observed how other systems, as the GPS and all means of information come together through this great IIC. This dynamic process of convergence of the ICT technological sectors together with the formation of a network of networks on the one hand gives place to the development of all "e-" services: e-commerce, e-government, e-health, etc.; while though on the other hand it inevitably sows fragilities. Hardware and software and adjoining programs are not, and perhaps will never be, fool- and error-proof.

Also, as many of the current technological risks do not respect national frontiers, there arise problems too, relative to regional or international coordination policies. The International Internet Connectivity (IIC), as defined for instance in the 'World Summit of the Information Society' in Tunis 2005, coordination and those of the IS as a consequence are by nature local, regional and global realities at the same time.

The trustworthiness of infrastructures, complex socio-technical systems and the trust that the citizen and society can deposit on them are at the core of the matter of IS governance. The advantages brought by the massive and ubiquitous use of ICTs may, concurrently become significant threats due to their security problems, at levels and extensions which are difficult to foresee as it is hard to predict the evolution of technologies and their future uses.

What is true is that, be it because of accidents with risk for physical or logical effects, destruction or decay of integrity or data disposability, failures or attacks affecting confidentiality, or the privacy of users the information society is destined to suffer continuous security problems.

Some of these problems will be accepted as minor and tolerable while others will cause major damage to people or companies, and, of course there will always be the possibility of exceptional events, though not impossible, with potentially catastrophic effects. This is the issue to be explored in this article.

From this point of view, the ITC is a critical infrastructure of the IS. Horrible failures in its functioning leading to the collapse of the technical base of the IS for a certain period will result in the loss of data transmission and access to sources of information thus affecting other critical infrastructures (water, transport, electricity, logistics) and could within days lead to the collapse of society.

The risk, concretely refers to the possibility of damage or harm in a given sector, for instance, the information and communication infrastructure together with the extension of this damage to all other infrastructures that depend upon the IS.

There are at least two perspectives about the risk: an objective one that can be measured and a subjective one, not only at personal level but also having social components, and referring to the perception of danger. The risk then does not refer exclusively to specific damage; on the contrary, it takes into account the consequences on society as a whole.

According to the International Risk Governance Council (2009; 2006) the risk of critical infrastructures must be thought about from the point of view of the consequences more or less certain from events or activities and from their potential impact regarding what is valuable be it for society as a whole, be for a group or for a single individual. As an example this can involve concrete things such as natural goods, the environment as a whole, human health, natural resources, etc. as well more abstract elements like social and economic stability, privacy, etc.

It must be born in mind that the inherent characteristic of risks is uncertainty and therefore, since risks are uncertain and contingent to many undetermined factors, it is difficult to foresee them in an analytical way or be based on statistical values. One of the main tasks is to imagine future scenarios, that is, the possible shapes these risks can adopt through a systematic study of possible future situations with the goal of better defining defensive and palliative strategies.

5.0 RISKS OF CRITICAL INFRASTRUCTURES AND DEVELOPING COUNTRIES

According to certain initiatives and to the experience of the most advanced societies that have gone deeper on this issues over the last decade, risks can be defined bearing in mind the 5 main systems of critical infrastructures: Supply of energy; Supply of drinking water; Treatment of waste; Transport; Information and communication infrastructure (that is digitally based including Internet, used for managing, monitoring and controlling the other infrastructures).

The "Critical Infrastructures" are a network of interdependent systems at great scale and imply complex physical transnational distributions associated to technologies and cybernetic networks, product of the interconnection with information and communication systems (Gheorghe et al., 2013; 2005). Here we can consider three main aspects:

a. Their function is to produce a continuous and universal flow of basic services which are essential for the economic and social development. In other words they are elements which have to be at everyone's disposal at all times. The user is not worried about the complexity present behind his access to the service; he wants just to be connected and that the service be available.

b. They tend not to be the possession of only one owner (public or private), operator or regulator or user, and have diverse functioning logics. After the process of opening of markets which took place in the world as from the 1980s, infrastructures were no longer seen as natural monopolies. The technological development has been used for opening up market infrastructures (see for instance, the process called "unbundling" of the European electricity system REF). Ideally, no single operator controls the infrastructure and when the systems are interconnected across borders, the very same national regulatory bodies see their powers being clipped.

c. They have been designed so as to satisfy basic social needs, but technological and organizational changes have raised their complexity and are bound by internal and external risks

due to intentional or accidental failures. When these failures do occur, they tend to propagate and exceed the structural, functional and territorial limits of each single system.

From the point of view of developing countries, some of the main elements to be considered as regards critical infrastructures are the following:

(i) The progress of paradox: more development leads to more fragility. Infrastructures are critical

The development of the economy has been determined in the 20th Century and at the beginning of the 21st Century by the growing incorporation of technologies improving productivity and innovation. This affected the industrial production of goods and services and the infrastructures supporting them. Their evolution is characterized by the massive integration of technologies, mainly information and communication and by the mutual integration and interdependence (for example, between transport systems, energy, financial and communications.).

In order to be competitive at the international level, it is essential to count with adequate means of transport, telematic access to markets, dependable energy supply, etc. Not to mention the same chains of supply necessary for production (e.g. fertilizers).

But, as it has been proved in regions like North America, Europe and Japan, the increase in infrastructures and their technological content makes them more fragile to all kinds of possible threats, be it with regards to loss of important capitals invested or to the damages that a decrease or perturbation of the infrastructural services or, the very destruction of the infrastructures and what this can provoke: good examples of these are natural risks, technical failures of systems, human errors in complex situations and probable fraudulent attacks such as terrorism, organized crime, radical groups, war (Ortiz, 2012; NIPP; 2009).

It is for this reason that developing countries must worry not only about the investment in the growth of their capacities in infrastructures but also in their protection and in recognizing their criticality and vulnerability.

Possible accidents, like Hurricane Katrina or an earthquake, or international conflict situations like the one in Estonia, Georgia or the Balkans which will affect the critical infrastructures might cause vital damage to society.

(ii) The management of infrastructures and their critical aspects requires a new kind of collaboration between public and private actors: system of governance

Over the last few years there has been a deep transformation in the management of infrastructures: from public services in the hands of the State,or in the hands of government bodies, generally in a situation of monopoly, to a kind of enterprise management, mainly in private hands and with a tendency to abide by economic market rules.

Infrastructures managers are therefore the main investors in these systems and resources, and they do so with a double objective: to satisfy the needs of social and economic actors served by this infrastructure (like in the case of drinking water, electric energy, etc.), but also to guarantee the continuity and the quality of services since the good functioning of society depends on this condition.

These guarantees are usually detailed in the contracts of allocation of the service. But, in an open market with many competitors and rapid technological evolution, and close and accented interrelations between infrastructures, it is not always evident what is the necessary level of protection and security. To leave such a delicate issue up to the will and decision of companies does not seem effective since investments in security and the trustworthiness of the service normally do not have an immediate return. In the case of several actors competing, it may occur that the different types of investment degenerates the balance of the markets. Examples of this are problems such as “free riders” and “moral hazards”.

In these cases the legitimate enterprise interests may be in conflict with society’s needs (even without considering enterprise fraud). In order to solve this, society needs a new approach to govern situations of public relevance but managed by the private sector.

The solution to this problem must consist of the implementation of new governance models with the participation of all actors involved. This also implies shared decision-making. This may be linked to the definition of standards (technical and belonging to processes), control procedures etc. The great challenge is to make compatible and synergic the market mechanisms and the strategies for the security of the state.

(iii) Critical infrastructure as crucial pivot for innovation

Infrastructures can be innovation engines from two different points of view. First, infrastructures constantly demand new products and services and also need new internal processes and in relation to his productive chains (suppliers, clients, etc.). This demand is materialized in relation to the elements necessary for the continuity and efficiency of operations, but also in relation to the security and dependability in the supply of services.

On the one hand, infrastructure operators have to invest in a continuous way in technologies in order to be able to produce in a profitable manner, seeking to keep being competitive in the market; and in order to respect different standards and norms (such as environmental for transportation and energy). They have to protect their infrastructures from various possible dangers and correct possible problems caused by the technologies (like software mistakes). On the other hand, if the infrastructures are qualified and competent, they may act as innovation catalysers offering new and better services at a better price.

This last point is particularly true in the case of information infrastructures with the developing of the IS. It is evident that Internet and mobile communications allow the growth of new industrial, commercial and public services capacities (e.g. e-government, e-health, e-commerce, etc.)

(iv) Critical infrastructures as comparative advantages: human resources

Infrastructures are designed, operated, maintained and used by qualified staff. The training of these persons is crucial for the efficiency and competence that can be obtained within the infrastructures. As many of the subjects involved are new, not always the academic institutions are prepared for satisfying the requirements of industry. No the least, many issues are multi-disciplinary, cutting across the vertical lines typical of the subjects offered in universities.

The most developed countries are already investing in the formation of technicians and professionals who will have responsibility over those infrastructures. This requirement not only refers to technical staff, but there is a need for lawyers, economists, etc.

6.0 GOVERNANCE AS A RESPONSE

There is one aspect of the problem on which all decision-makers agree upon: risk must be managed and controlled, but how? Living with risk confronts contemporary societies with questions of a political character. Here is where governance comes in.

Governance can be understood as the structure and processes for a collective decision involving government and non-government actors. (Nye and Donahue, 2000).

The EU has defined in its white book about principles for good governance. They must be applied to the specific case of identification, evaluation, management and communication of risks. Amongst other principles, governance presupposes the participation of all political, economic, social and scientific-academic actors in consulting aspects, starting from a bigger sense of responsibility in the decision making and the participation of citizens in the elaboration and application of policies .It requires transparency in the communication of decisions and efficacy regarding the taking of decisions in scale and at the appropriate moment.

Risk governance refers to the capacity of organizations and people to face inevitable risks (Aven and Renn, 2010). As a management tool it refers to processes oriented to the taking of decisions where comprehensive, whole solutions can be defined and found for all relevant actors with interests and who are involved in the particular subject (stakeholders). It is in this sense that

governance is a process of participation and consulting useful for managing complexity. The idea is that only the management of complexity can reduce complexity.

A very important example of the new risks and of risk management in a regional context through governance mechanisms is given by the crisis in the interconnection European electrical system in 2004.

The teaching from this experience reveals that in the contemporary world there is a continuous widening of the threat spectrum and that it must be faced by all infrastructures, including critical ones; this includes a variety of natural occurrences, technical failures and accidental or intentional human actions which challenge the stability of networks and the safety of some services which should never be interrupted.

The point is that when the whole functioning depends on one complex technological system, one single failure may have catastrophic consequences (Renn, 2008).

An adequate risk management in critical infrastructures has the advantage of:

- Reducing the growing interdependency in the negative aspects of crisis transmission.
- Promote the management of the demand and the adjustment of priorities.
- Reduce the times for restoring the system after a failure and allows for the maintenance of critical social services when facing a failure in the system.

7.0 HEMISPHERIC STRATEGIES FOR THE PROTECTION OF CRITICAL INFRASTRUCTURES (PCI) AND THE CYBER SECURITY IN THE AMERICAS

Different agreements celebrated during the last years by the countries of the Organization of American States (OAS) settle the basis for the strategies of PCI and cyber security:

- The Hemisphere faces an increasingly diverse and complex set of threats and "challenges for the states, societies and people" and there are "particular strategic context of each sub-region in the Hemisphere", the civil and civil-military cooperation in the fields of Defense and Security is necessary. V Ministers of Defense of America Conference (Santiago de Chile, November 2002).

- The new concept of security in the Hemisphere is multidimensional in scope, and includes traditional and new threats, concerns, and other challenges to the security of the states of the Hemisphere, incorporating the priorities of each State. The security of States of the Hemisphere is affected, in different ways, by traditional threats and the following new threats, concerns, and other challenges of a diverse nature and it includes "attacks to cyber security" and consider "new terrorist threats, whatever their origin or motivation, such as threats to cyber security, biological terrorism, and threats to critical infrastructure" OAS, Declaration on Security in the Americas (OAS, 2003).

- An Inter-American Strategy to Combat Threats to Cyber security. "A multidimensional and multidisciplinary approach to create a culture of cyber security" to protect de infrastructure of the telecommunications and give responsibilities to the Inter-American Committee against Terrorism (CICTE) for a formation of an Inter-American Alert, Watch, and Warning Network to Rapidly Disseminate Cyber Security Information and Respond to Crises and creation of the hemispheric network of a Computer Security Incident Response Teams (CSIRTs).

-Inter-American Telecommunications Commission (CITEL): for the identification and Adoption of Technical Standards for a Secure Internet Architecture (OAS, 2004).

This important document is a key to consider firstly a common vision of the Critical Infrastructures in the Americas.

-Hemispheric definition of Critical Infrastructure (CI) "refers, among others, to those facilities, systems, and networks, and physical or virtual IT services and equipment, the disabling or destruction of which would have a severe impact on populations, public health, security, economic activity, the environment, democratic governance, or the ability of the government of a Member State to operate effectively" (OAS, 2007). This important document is a key to consider firstly a common vision of the CI in the Americas.

-Trends of Cybersecurity in Latin America and the Caribbean. These first general mapping of the cybersecurity in Latin America show that the region features a youthful population craving

more online access. The recent situation regarding cyber threats in Latin America and the Caribbean shows that users are suffering the impact of threats that are prone to global level and others specific to each region. As an aggravating factor of this challenge, Latin America and the Caribbean have the fastest growing population of Internet users of the world, with an increase of 12 percent during the last year. This report identified the main trends that impact the region: the weak capabilities of law enforcement agencies, and the complex forms and scale of crime online (OAS, 2014).

8.0 SOME LESSONS FOR LATIN AMERICA (POINTS TO BEAR IN MIND)

Latin America must have an active participation in the construction of the IS. The aim is to "incorporate the paradigm of the IS in the development agenda"; even more so when there is an attempt to re-launch the program on the development of infrastructures in the plane of intra-South American relations. A true conception of regional integration cannot leave behind the question of infrastructures and that of the associated risks to this process. It cannot be forgotten that new threats and vulnerabilities appear from the crossing between new information technologies and the communication with infrastructures (Girard and Perini, 2013).

These are some of the ideas that synthesize the perspective of this work:

(1) The diverse issues that appear from the construction of the IS will internally influence the definition of the quality of life, wellbeing and growth projection of citizens; internationally, it will influence the definition of interests in foreign policy, in the regional integration processes and the general behaviour of the region.

(2) In the IS, the objective should be to develop means and capabilities, and to have better infrastructure with an adequate use of technology- But it should be always taken into account that this carries along fragility, and so the potential benefit has a strong interconnection with the potential negative effects. The challenge of a good risk management rests then on the utilization of the benefit of information and communication technologies while minimizing the negative consequences associated with the risks.

(3) It is absolutely necessary to have risk management of regional or global character, especially of those that have a high level of impact on health, security, the environment, the economy or society- In addition, these should be evaluated and managed through widely participative consulting mechanisms. This means that the development-risk duality needs to be analyzed by the diverse interested and committed publics (stakeholders), and also it must be included as a variable by formulators of policies and managed by political authorities.

(4) Infrastructures are operated by companies (private or public, but with a business organization and a search for profit). Therefore, there is a need for governance as a management tool at the different levels of territoriality and particularly applied to the integrated management of multiple actors, multiple interests and perspectives. Risk governance is the only modality which allows the convergence of the interests of companies with the requirements and integral demands of a society.

(5) The specific risk in critical infrastructures has to be considered as object of analysis. Security in the supply of the service and the impact that might occur if there were any long interruption of the services, should constitute a high level priority for legislation, coordination of policies, planning and the evaluation of scenarios.

(6) The global risks are not contained within national borders and therefore, cannot be managed through actions or policies by just one sector or isolated government. Thus, risk governance, especially those of regionally interconnected critical infrastructures, requires a special coordination among the countries that may be involved.

(7) From the perspective of the socio-economic implications, infrastructures in their fast evolution "consume" products and services at the same time that they show the way to new social and economic capacities. This situation defines the field of development: for instance: What sort of energy is produced and how is nuclear energy used versus new sources? How many companies can generate and distribute energy? The effects on the working structure must be evaluated. The studies

about the need (and the opportunity) for human resources with new technical and professional abilities, that is, through the widening of competences and labour skills in a new context of the development of the social and human capital.

(8) More theories about international relations and regional cooperation-integration must be generated. It is true that the nation-state is pulled apart by different demands and requirements, but it is also true that the State in the IS will have to fulfil new functions and generate widened capacities in a scenario of growing complexity. In a word, there are two issues combined here: (i) the IS, risks, threats and vulnerabilities, critical infrastructures, implementation of mechanisms and governance policies all under a sustainable development focus, and (ii) the international dimension, as they will be, over the next few years issues of great interest for the majority of countries and will be included in public and private agendas.

9.0 CONCLUSION

The central idea is that we have entered an era of complexity where instability, uncertainty and turbulence are not merely exogenous and circumstantial variables but also structural features of the system. This complexity cannot be studied in an abstract way when studying its harmful effects and, in particular, the risks induced by it.

The international context also presents deep asymmetries which considerably influence the intensity of the risks and the means used to counter them. This situation can be measured not only by the unequal levels of relative development or by the high concentration of the fruits of technical progress in developed countries, but also by the diverse capacities societies may have to respond to this complexity, as has been proven by some CEPAL-United Nations studies. It is clear from what has been exposed here, that the risks of infrastructures must be analyzed bearing in mind the social, political and economic characteristics specific to each community being studied.

In the Organization of Americans States (OAS) the countries of Latin America and North America agree a common vision of the risks and threats in the cyberspace and the firsts lines to protect and reaction the Critical Infrastructures physical and informational (virtual) against it. In Latin America this situation requires as an answer the elaboration of national, bilateral or multilateral policies and strategies to create strong capabilities. In the Region it is necessary firstly to secure Critical Information Infrastructures.

One of the fundamental issues in contemporary society is related to the matter of how to take decisions in matters concerning the whole of the social system. And, that these decisions might carry along negative aspects that could affect diverse social groups in different modes and degrees be it geographical, economic, educational and age aspects, etc.

It must also be considered that problems are multidimensional: there is a diversity of aspects and factors such as legal, economic, social, political, financial, health, psychological, environmental, technical… and then there are risks that accumulate with the passing of time. This is why there should always be options: there is no single way forward. Issues are difficult to solve and many questions require a deep societal and governmental awareness: who is responsible, who pays, who criticize, who takes decisions and how and above all, how the scientific base is used.

"Uncertainty is inherent in all stages of risk assessment". Truly, according to what is maintained in recent studies about decision making, it is a problem of processes and institutions, of efficiency but also of precaution, trying to understand what are the potentialities and the limitations of the method and the evidence being employed. Both, processes and institutions must be designed for the objectives of risk analysis in a given situation.

Finally, it must be emphasised that one of the tasks to be developed is that of the rational thinking that is scientific, including knowledge, instruments and technologies, which will allow us to analyze, interpret, identify and manage risks. This may be the most important competitive advantage in the 21st Century together with financial and engineering capacities (amongst others) for the design, development and direction of these infrastructures.

REFERENCES

Aven, T. and O. Renn (2010). *Risk Management and Governance. Concepts, Guidelines and Applications*, Berlin, Springer Verlag.

BBC (2007). Estonia hit by 'Moscow cyber war'. BBS News. One-Minute World News, 17 May 2007.

Beck, U. (1992). *Risk Society. Towards a New Modernity*. London, Sage.

Bernal-Meza, R. y G. Masera (2007). "Sociedad de la información: etapa posterior de la globalización", *Realidad Económica*, Nro. 227, pp. 90-116.

Bevir, M. (edit.) (2007). *Encyclopedia of Governance*. London, Sage.

Bischoff, H.J. (2008). *Risks in Modern Society*. Dordrech, Springer.

Campbell, S. (2007). 'Risk and the Subjectivity of Preference'. *Journal of Risk Research,* Volume 9, 2006 - Issue 3, p. 225-242.

Castells, Manuel (2002). *'Net war,' Diario El País, Madrid*, Spain, 6/02/02.

Castells, Manuel (1998). *'Net State?': Economic and political Globalization in the information age',* Society and State Reform, San Pablo, march, 1998.

Cepal (2003). *Los Caminos Hacia una Sociedad de la Información en América Latina y el Caribe*, Santiago de Chile, UN-CEPAL, Documento de Bávaro.

Comisión Europea (2003). *Hacia la Europa basada en el conocimiento. La Unión Europea y la sociedad de la información*. Luxemburgo: Oficina de Publicaciones Oficiales de las Comunidades Europeas.

Gheorghe, A. et. al. (2005). *Critical Infraestructures at Risk*, Dordretch, Springer.

Gheorghe, A.,M. Masera, and F.Polinpapilinho (edits.) (2013). *Infranomics. Sustainability, Engineering Design and Governance*, Dordrech, Springer.

Girard, B. and F. Perini (eds.) (2013). *Enabling Openness: The future of the information society in Latin America and the Caribbean*. Otawa: Canada, IDRC.

Hadkiewicz, W. and P. Gawowicz (2013). "Information technologies in the postindustrial society". *Procedia - Social and Behavioral Sciences*, Elsevier, N°103: p. 500 – 505.

International Telecommunications Union [ITU], (2006). *WSIS Golden Book*, Geneva, United Nations.

International Risk Governance Council [IRGC] (2006), *White Paper on Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures*, Geneva.

International Risk Governance Council [IRGC] (2009). *Risk Governance Deficits*
An analysis and illustration of the most common deficits in risk governance. Geneva.

International Risk Governance Council [IRGC] (2010). *Emerging risks. Sources, drivers and governance issues*, Geneva, Revised edition.

International Risk Governance Council [IRGC] (2016). *Workshop Report. Cyber Security Risk Governance.* Geneva. Swiss Re Centre for Global Dialogue, Zurich, Switzerland 29 – 30 October 2015.

Keyworth, G. (1998). *The Digital State: How State Governments are Using Digital Technology*, Washington, DC. The Progress and Freedom Foundation, September 1998. .

Lechte, J. (2003). *Key Contemporary Concepts*. London, Sage.

Lippert, T. H. (2016). NATO, Climate Change, and International Security: A Risk Governance Approach. Santa Monica, CA: RAND Corporation, 2016.

Mansell, R. (edit.) (2009). *The Information Society. Critical concepts in sociology.* London and New York, Routledge.

Masera, G. (2008). "Impactos en la Sociedad Global de la Información", *Políticas Públicas*, FAE-Universidad de Santiago de Chile, vol.2, nro. 1, pp. 5-27.

Masera, G. (2010). *Epistemología y Economía Mundial*, Mendoza, EdUDA.

Mythen, G. (2004). Ulrich Beck. *A Critical Introduction to the Risk Society*. London, Pluto Press.

NIPP (2009). *National Infraestructure Protection Plan*. US Department of Homeland Security.Washington D.C., U.S. Department of Home Security.

Nye, J. and J. Donahue (edits.) (2000). *Governance in a Globalizing World,* Washington, D.C., Brookings Institution.

OAS (2003). Declaration on Security in the Americas, Mexico City, 28 October 2003.

OAS (2004). *Adoption* of a *Comprehensive*. *Inter-American Strategy* to *Combat Threats* to *Cybersecurity*: *A Multidisciplinary Approach to* Creating a Culture of *Cybersecurity.* Washington DC.

OAS (2007). *Declaration on the Protection of Critical Insfrastcture in the Hemisphere in the Face of Terrorism*. Inter-American Committee against Terrorism (CICTE), Panama City.

OAS (2014). *Cybersecurity trends in Latin America and the Caribbean,* Washington DC.

OECD (2003). *Emerging systemic risks in the 21st Century – An Agenda for Action*, Paris; International Futures Project.

Ortiz, J. (2008). *«Argentina the Challenge of the information operations»*. *The World Views IO*. IO Sphere. San Antonio TX, Special Editon 2008, p. 57-63.

Ortiz, J. (2012). "Estrategia de Defensa Cibernética en la era de la información", *Revista de la Escuela Superior de Guerra del Ejército Argentino*, N° 582, (Septiembre-Diciembre), p. 89-112.

Peres, W. y M. Hilbert (eds.) (2009). *La sociedad de la información en América Latina y el Caribe*. Santiago de Chile, Naciones Unidas-CEPAL.

Pierre, O. and G. Peters (2005). *Governing Complex Societies. Trajectories and Scenarios*. New York, Palgrave Macmillan.

Renn, O. (2008). *Risk Governance. Coping with Uncertainty in a Complex World.* London, Esarthscan.

Saadawi. T. and L. Jordan (edit.) (2011). *Cyber Infrastructure Protection*. PA: USA, Strategic Studies Institute.

Thomas, Timothy L. (2005). *Ciber Silhouettes: Shadow Over Information Operations*, Foreign Military Studies Office, KS.

Thompson, P. (1990): "Risk Objectivism and Risk Subjectivism: When Are Risks Real?", *Risk: Health, Safety & Environment*, n°1: 3, (January), Article 4, p. 3-22.

Webster, F. (2002). "The information Society Revisited", in L. Lievrouw and S. Livingstone (Edit.). *Handbook of New Media, Social Shaping and Consequences of ICT's.* London, Sage, 2002, p. 22-33.

Webster, F. (2006). *Theories of Information Society.* London and New York, Routledge, third edition.