Gobernanza de riesgos en la sociedad de la información

Gustavo Alberto Masera[1] **& Javier Ulises Ortiz**[2]

Resumen

El propósito de esta investigación fue analizar los riesgos que conllevan los cambios tecnológicos, especialmente los relacionados con la aplicación de las tecnologías de la información y de la comunicación. Se utilizó como método principal la identificación de tendencias relevantes en el ámbito internacional, mediante una revisión de los documentos elaborados por los organismos internacionales y *think tanks*, junto a la consulta a obras especializadas. La tesis sostenida en el documento plantea la necesidad de comprender el riesgo sistémico, así como el que se encuentra directamente asociado al desenvolvimiento de las infraestructuras críticas. El resultado del trabajo concluye que el riesgo es inherente a la expansión de la compleja sociedad de la información y que el mismo conlleva un aumento considerable de las vulnerabilidades emergentes del sistema social. Se argumenta que la gobernanza es un proceso orientado a la toma de decisiones colectivas en una sociedad; y en tal sentido, se torna en uno de los principales mecanismos para la gestión del riesgo. La gobernanza permite enfrentar los desafíos que presenta la brecha tecnológica en los países en vías de desarrollo, y en América Latina en particular.

Palabras claves: sociedad de la información, nuevas tecnologías, riesgos, infraestructuras críticas, gobernanza.

[1] FING-UNCuyo; IDICEJ-Universidad del Aconcagua (Mendoza, Argentina).

[2] Instituto Universitario del Ejército (IUE - Buenos Aires, Argentina).

Fundamentos y objetivos de la investigación

La percepción compartida por los analistas subraya que los cambios científico-tecnológicos que han tenido lugar desde las últimas décadas del siglo XX constituyen a la vez un desafío teórico –dada su complejidad y su dinámica en estado de flujo- y un campo de oportunidades para el desarrollo económico, político y cultural. Al mismo tiempo, en la medida en que se vincula con los impactos del proceso de globalización, estas transformaciones a ritmo acelerado, representan un conjunto de amenazas para la sociedad como sistema, como sucede, por ejemplo, con los desastres tecnológicos.

El tema tiene un inicio simbólico con la serie de explosiones que destruyeron el reactor de la central eléctrica atómica de Chernobyl. En efecto, la crisis socio-ambiental iniciada en abril de 1986 en Ucrania y esparcida por distintos países marca el inicio de una nueva época: la de los riesgos globales (Alexievich, 2006).

El objetivo del trabajo es identificar los principales riesgos emergentes en la sociedad de la información. Esta labor, de carácter introductoria, facilita la evaluación de aquellos potenciales que específicamente surgen en las denominadas "infraestructuras críticas". Se concluye que dado que los eventos pueden impactar decisivamente en el bienestar y el funcionamiento de una sociedad, su gestión mediante la gobernanza de riesgos se convierte en un aspecto crítico para las sociedades.

Respecto al método, se ha tomado en cuenta: 1) la experiencia de los países industrializados, según lo revelan documentos de organizaciones (nacionales, internacionales, *think tanks*); 2) la combinación de líneas de investigación, programas académicos y obras especializadas. A fin de contextualizar el conocimiento en el horizonte regional, se derivan lecciones y desafíos para América Latina.

Sociedad de la información: raíces de un concepto

En los últimos años, el concepto "sociedad de la información" (SI) se ha difundido por el planeta, en gran parte debido a la notable expansión del sector info-comunicacional, ayudado por las numerosas iniciativas en el ámbito internacional, que han tenido por objeto su análisis y su promoción. Así, su utilización se generalizó con el reconocimiento oficial otorgado por las "Cumbres Mundiales sobre la Sociedad de la Información" (WS-SI), coordinadas por Naciones Unidas, a través de

la Unión Internacional de Telecomunicaciones (ITU, 2006) y cuya primera Conferencia se realizó en Ginebra en el 2003.

El establecimiento de un área especial sobre SI, por parte de la Comisión Europea, también impulsó su utilización. Igualmente, el término SI es discutido (Webster, 2002), y por lo mismo se han propuesto alternativas, aunque no exactamente equivalentes: entre ellas, sociedad postindustrial (Bell; Masuda), sociedad digital (Mercier, Plassard, y Scardigli) y sociedad en red (Castells; van Dijk), han tenido mayor repercusión, tal como revela el itinerario de teorías elaborado por Webster (2006) y Mansell (2009).

Aunque desde hace tiempo se habla de "sociedad del conocimiento" (Böhme and Stehr, 1986), se considera que ésta sería, en realidad, una etapa posterior a la SI y como una consecuencia del ingreso al mundo BING. El significado del acrónimo muestra que el aspecto decisivo del paso de una fase a la otra, se encontraría en la posibilidad de dominación más intensiva de los campos biológicos, informáticos, nanotecnológicos y el de las ciencias del comportamiento y neuronales (*behavioral and neural sciences*) (Bernal-Meza y Masera, 2007).

La SI se la define como un estadio del desarrollo caracterizado por la capacidad de sus miembros para obtener y compartir cualquier información, instantáneamente, desde cualquier lugar y bajo diversas formas. El factor de posibilidad es la aplicación universal de tecnologías homogéneas de procesamiento y comunicación de datos, conectadas mediante autopistas de la información. La SI hace referencia, entonces, a un nuevo paradigma, cuyos criterios orientadores dan cuenta del camino hacia un tipo de sociedad en construcción, resultante de la acción de los nuevas tecnologías y de los progresivos procesos de digitalización (Cepal, 2003; Peres y Hilbert, 2009).

Por nuevas tecnologías se entiende el conjunto convergente de tecnologías en microelectrónica, robótica, redes, autopistas de la información, computación (máquinas y software), telecomunicaciones, transmisiones y optoelectrónica; a las que se agregan las aplicaciones tecnológicas y de ingeniería derivadas de la ciencia de materiales, incluyendo los mecanismos de coordinación que permiten manipularlas. (Hadkiewicz and Gawowicz, 2013).

La fuerza conductora de este estadio del desarrollo, son específicamente, las nuevas tecnologías de la información y de la comunicación (TIC). Una consecuencia directa es que su uso masivo genera

una mayor interdependencia, dada la propensión a utilizar la misma tecnología o similares en todo el orbe. En este sentido, son las verdaderas herramientas de la globalización, porque posibilitan una mayor: a) velocidad de transmisión en tiempo real o instantaneidad; b) conectividad entre actores mediante autopistas de la información y redes, lo que deriva en un aumento del grado de densidad en las relaciones sociales; c) intangibilidad de la información digitalizada en forma de textos, imágenes, voz; d) aceleración e intensificación de los flujos de intercambio (Masera, 2010).

El aspecto decisivo de la SI se encuentra en el potencial de digitalización, en las formas de comunicación y en la capacidad de los individuos para obtener y compartir cualquier información, instantáneamente, desde cualquier lugar y bajo diversas formas, gracias a la aplicación universal de tecnologías homogéneas tanto de procesamiento como de comunicación de datos. La digitalización supone el uso intensivo de varias clases de ordenadores y otras tecnologías, en una labor de modelización de acuerdo a determinadas operaciones, junto con la fase de innovación vinculada a la creación y puesta en funcionamiento de toda una serie de infraestructuras (Rennstich, 2008).

Riesgos en la sociedad de la información

En los inicios de la postguerra fría, Ulrich Beck (1992) introdujo el concepto de "sociedad del riesgo". Téngase en cuenta, tal como se ha ya mencionado, que pocos años antes había ocurrido el caso más emblemático sobre la fragilidad de los sistemas tecnológicos. El accidente de la planta nuclear de Chernobyl en la antigua Unión Soviética reveló el límite de la modernidad (Lechte, 2003).

Beck argumenta que la verdadera naturaleza del riesgo ha cambiado. Sostiene que la tecnología actual ha creado nuevas formas de riesgo e impone una peligrosidad cualitativamente distinta a la del pasado. El riesgo ha dejado de ser contingente para convertirse en un rasgo estructural del nuevo orden de cosas y, además, hacia fin de siglo, el riesgo ha pasado a tener secuelas sobre un área geográfica más extensa y crecientemente global. Beck señala problemas y critica las limitaciones de la sociedad actual, donde los accidentes no pueden ser aislados (como el cambio climático), aunque no llega a proponer un modo para gestionar esos problemas. A pesar de ello, su valoración del riesgo social ha sido muy influyente y ha permitido profundizar los debates sobre

el diálogo político en torno a temas claves: ambientales, alimentarios, energéticos, etc. (Mythe, 2004). En análisis más recientes (p.e. Bischoff, 2008), junto a una más precisa determinación de amenazas y fallas potenciales, de sus causas y consecuencias, se ha avanzado en la elaboración de perspectivas intersectoriales; incluso se asiste al nacimiento de una nueva área de conocimiento (p.e. *Infranomics* como disciplina de disciplinas), de las que se derivan modelizaciones, instrumentos y prácticas (Gheorge Gheorghe, Masera and Polinpapilinho, 2013).

En el mundo globalizado aparecen riesgos sistémicos por su impacto sobre el conjunto de la sociedad; los que, incluso, pueden desarrollar un contagio internacional. Aunque no hay una definición aceptada universalmente, sin embargo, se han clasificado dos posibles categorías de riesgo (Arven and Renn, 2010): aquellas donde el riesgo se expresa mediante probabilidades de un suceso aunado a valoraciones sobre expectativas; y las otras, que sostienen que los riesgos se expresan fundamentalmente por la ocurrencia de eventos imprevistos y las consecuencias que pueden emanar de los mismos, con un fuerte componente de incertidumbre. De acuerdo con lo expuesto, puede afirmarse que la noción de riesgo se refiere, en suma, a la incertidumbre acerca de la gravedad de las consecuencias (o resultados) de una actividad, con respecto a algo que la sociedad percibe como valioso, vital o crítico.

Thompson (1990) distingue entre riesgos reales, riesgos observados y riesgos percibidos. Los reales se refieren a lo que puede ocurrir, con consecuencias negativas y que pueden suceder con una probabilidad conocida por estadísticas (sismos, caídas de aviones). Mientras que los observados se pueden deducir de modelos, por ejemplo, sobre los posibles efectos de una epidemia. Los percibidos son juicios subjetivos que se emiten en la ausencia de modelos o conocimiento previo. Algunos factores que se tienen que considerar cuando se habla de riesgos son: a) incertidumbre sobre la probabilidad de ocurrencia; b) incertidumbre sobre la severidad del impacto de un fallo catastrófico; c) existencia de posibles víctimas y daños; d) reversibilidad de los efectos negativos; e) compensación por la exposición al riesgo; f) beneficios, peligros y costos para los distintos actores.

Dentro del ámbito general de los riesgos es necesario considerar aquellos específicos que se dan en el contexto de la SI. Se parte del reconocimiento de que ningún sistema socio-tecnológico es perfecto. En la SI, en particular, aparecen riesgos, amenazas y vulnerabilidades (y los puntos cercanos de errores, fallos, seguridad, etc.) antes desconocidos.

Sumado a ello, irrumpen antagonismos que demandan estrategias defensivas (Ortiz, 2012); entendiendo la diferencia entre ciberguerra (*cyberwar – information warfare*) (Saadawi, and Jordan, 2011); en cuanto a operaciones militares y netguerra (*netwar*): acerca de conflictos a gran escala entre naciones o sociedades comerciales (Arpagian, 2009).

El desafío se encuentra en que debe afrontarse rápidamente la cuestión de los puntos débiles que aparecen al conectar "todo", es decir comercio, gobierno, hospitales, bancos, energía, etc., a a la denominada "Infraestructura de la Información y de la Comunicación" - IIC (según la Cumbre Mundial WSIS – Fase de Túnez). Esta IIC es el soporte básico que hace posible la construcción de la SI, como el resultado de la interconexión de los sistemas de telefonía fija y móvil, con Internet, y las comunicaciones por satélites. Se ve como otros sistemas (por ejemplo, el GPS de posicionamiento global y todos los medios de comunicación) confluyen y se ven integrados por esta gran IIC. Este proceso dinámico de convergencia de los sectores tecnológicos TIC junto a la formación de una red de redes por una parte da lugar al desarrollo de todos los servicios "e-": *e-commerce*, *e-government*, *e-health*. Al mismo tiempo, implanta fragilidades puesto que los sistemas de hardware, software y procesos adjuntos no son, ni lo serán quizás, a prueba de fallos.

Los riesgos pueden derivarse de numerosos factores y en distintos ámbitos: *cracks* financieros; crisis alimentaria; calentamiento global; aumento de la desertificación; estancamiento de las negociaciones comerciales; problemas de suministros de gas y restricciones energéticas; renovados conflictos geopolíticos; fallas en los sistemas, como *blackouts* eléctricos de grandes dimensiones (Aven and Renn, 2010; OECD, 2003).

Infraestructuras críticas

Las sociedades contemporáneas descansan sobre numerosas y variadas infraestructuras.

La infraestructura es un sistema socio-tecnológico de segundo orden (sistema de sistemas), que cumple con un servicio vital, como es transmitir o transferir un flujo de algo (bienes, información, etc.) entre los nodos del sistema (Gheorghe et al., 2005). Particularmente, las "Infraestructuras Críticas" (IC) son una red de sistemas interdepen-

dientes de gran escala, y que implican complejas distribuciones físicas transfronterizas asociadas a tecnologías y redes cibernéticas, producto de la interconexión con los sistemas de tecnologías de la información y comunicación (Gheorghe et al., 2005).

La Oficina de Protección de la Infraestructura Crítica de los Estados Unidos (EUA) las definió como los sistemas que tienen incapacidades, o podrían ser debilitados o destruidos, generando impactos sobre la defensa y la seguridad económica de una nación, incluyendo bancos, transporte, sistemas de agua, servicios del gobierno y gobiernos públicos. Sobre esa concepción se han desarrollado estrategias para asegurar el ciberespacio y la protección física de las IC (NIPP, 2009) o la asociación para la seguridad de las IC y la "resiliencia" (Canadá, 2014).

La Unión Europea definió a las IC como aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados miembros (Comisión Europea, 2004). Por los expuesto, se desarrolló desde 2006, el Programa Europeo de protección de las IC (PEPIC).

Los principales sistemas de IC son: 1) energía (centrales y redes de energía); 2) abastecimiento de agua (embalses, almacenamiento, tratamiento de agua potable y redes); 3) tratamiento de desechos; 4) transporte (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico); 5) infraestructura de la información y comunicación, que incluye las tecnologías de base digital e internet, usadas para gestionar, monitorear y controlar las otras infraestructuras. Además, hay consenso en que las IC pueden incluir las siguientes área: instituciones financieras; sector sanitario; alimentación; producción, almacenamiento y transporte de mercancías peligrosas (materiales químicos, biológicos, radiológicos y nucleares); administración (servicios básicos, instalaciones, redes de información; etc. (Ortiz, 2012).

En las IC se pueden enumerar tres aspectos principales:

1. Su función es la de producir un flujo continuo y universal de servicios básicos que resultan esenciales para el desarrollo económico y social. En otras palabras, son elementos que tienen que estar disponibles para todos, en todo momento. El usuario no se preocupa de la complejidad detrás de su acceso al servicio, puesto que le interesa solamente conectarse y que el servicio esté disponible.
2. Las infraestructuras tienden a no ser posesión de un único dueño (público o privado).. Además, puede pasar que cada operador, regulador y usuario posean distintas lógicas de funcionamiento. La regionalización de los mercados, por ejemplo en la Unión Europea, ha conducido al "desacople" de su sistema eléctrico (*unbundling*), donde ningún operador controla la infraestructura de producción o distribución. Entonces, cuando los sistemas se interconectan a través de las fronteras, los mismos entes nacionales ven recortados sus competencias.
3. Las infraestructuras han sido diseñadas para satisfacer necesidades sociales básicas, pero los cambios tecnológicos y organizativos han elevado su nivel de complejidad, quedando sujetas a riesgos internos y externos debido a fallos accidentales o intencionales. Y cuando se producen fallos, éstos tienden a propagarse excediendo los límites estructurales, funcionales y territoriales de cada sistema singular.

Riesgos en infraestructuras críticas

La idea que recorre este apartado es que existe una relación directa entre infraestructuras críticas (IC), nuevas tecnologías (TIC) y sociedad de la información (SI). Por consiguiente, un conjunto de fallos en el funcionamiento de las TIC, pueden hacer colapsar por un cierto período la base técnica de la SI, y ello resultará en la pérdida de transmisiones de datos y del acceso a fuentes de información, afectando otras IC (agua, transporte, electricidad, logística, aeropuertos), lo que en pocos días derivará colapsando la sociedad misma.

El riesgo, en este nivel específico, implica la posibilidad de daño o avería en un sector determinado, por ejemplo, la infraestructura de la

información y de la comunicación (ICC), conjuntamente con la extensión de este daño a todas las otras infraestructuras que en la sociedad de la información dependen de ella (IRGC, 2006).

Hay diversos casos testigos de los riesgos que se presentan a las IC. En uno, pueden darse los posibles fallos en las TIC (sistemas operativos, programas de ofimática, cortes masivos de energía eléctrica), y la posibilidad de "cyberataques" a Estados en su totalidad. En otro, puede revelarse la fragilidad de los sistemas de seguridad de determinadas instalaciones. En ambos casos, las nuevas tecnologías se asientan o impactan sobre el espacio urbano donde se estructuran los nodos de IC dadas por el complejo tecnológico-electrónico-informacional. Debe reflexionarse sobre la logística que supone sostener los requerimientos de subsistencia de las grandes concentraciones urbanas y la administración de sus recursos. Es que la concentración urbana crea un nuevo espacio "las megalópolis", constituyéndose en ellas sistemas "meta estables" que las sostienen, y por ello, verdaderamente sustanciales (Ortiz, 2012).

Los riesgos pueden incidir en las IC de una sociedad, afectando la estabilidad política y la prosperidad económica de los países. Además, son procesos que pueden generar cambios en la distribución del poder entre los países, así como efectos catastróficos en regiones vulnerables.

En lo que respecta a los desastres naturales, los terremotos y tsunamis han afectado a todas las civilizaciones en las diversos períodos históricos. La diferencia en la actualidad, es que las consecuencias podrían ser más desastrosas aún, por la difícil continuidad de la vida cotidiana luego de la destrucción de las infraestructuras básicas. Los ejemplos sobran: Nueva Orleáns, posteriormente al huracán Katrina; Haití después del terremoto; Japón, seguidamente a los problemas de la central nuclear de Fukushima, etc. Estos casos evidencian la sensibilidad y el riesgo que representa el impacto sobre las IC. Al mismo tiempo, dan la impresión de que la sociedad se encuentra al borde de perder el control de frente a un número importante de riesgos, amenazas, desastres y crisis no convencionales.

Según el *International Risk Governance Council* (2010), que toma la definición de Riesgo de Arven y Renn, el riesgo de las infraestructuras críticas debe ser pensado desde las consecuencias más o menos inciertas de un evento o de una actividad, y desde su potencial impacto en temas críticos, ya sea para la sociedad en su conjunto, ya sea para un

grupo o un individuo concreto. Esta ponderación puede comprender cosas como los bienes naturales, el ambiente en su conjunto, la salud humana, los recursos naturales, etc., como elementos más abstractos como la estabilidad social y económica, la privacidad, etc. A pesar de que es difícil prever los riesgos, una de las tareas implicar imaginar escenarios futuros, posibles vías que puedan adoptar, mediante un estudio sistemático de situaciones futuribles, con la finalidad de definir las mejores estrategias paliativas.

El reconocimiento de la importancia de las IC se ha propagado por las principales potencias del sistema internacional. Rusia, a partir de la Organización del Tratado de Seguridad Colectiva (OTSC) de la Comunidad de Estados Independientes (CEI) con China, y en conjunción en el marco de la Organización de Seguridad y Cooperación de Shanghai (OCS) han comenzado a crear mayores capacidades de protección de sus IC. Pero, las IC rusas que aportan energía a Europa, presentan riesgos que potencialmente afectarían la seguridad de los suministros energéticos (Arteaga, 2010). Las presentes situaciones conflictivas en Ucrania-Crimea, Siria-Irak, Afganistán, etc. son una clara evidencia de lo que se llama riesgos a la "seguridad de los corredores energéticos" (Palma, Masera y Echegaray, 2014).

En el ámbito regional, en el seno de la OEA, se estableció en 2004 un consenso generalizado con el establecimiento de la llamada "Estrategia Interamericana integral para combatir las amenazas a la seguridad cibernética". Es un enfoque multidimensional y multidisciplinario dirigido a la formación de una cultura de seguridad cibernética, para proteger la infraestructura de las telecomunicaciones, redes y sistemas de información. Posteriormente, la misma OEA propició la creación de una "Red Interamericana de Seguridad Cibernética" (2005), a partir de los grupos nacionales de "vigilancia y alerta", también conocidos al presente como los "Equipos de Respuesta a Incidentes de Seguridad en Computadoras" (CSRITs), cuyos objetivos son: a) identificar y luchar contra las amenazas, independientemente de su origen y motivación; b) formular planes nacionales de respuestas a situaciones de emergencia; c) crear una red interamericana de vigilancia y alerta para diseminar rápidamente información sobre seguridad cibernética y responder a crisis, incidentes y amenazas a la seguridad en computadoras.

La Gobernanza en un contexto de riesgos

Existe un aspecto del problema en el que los especialistas están de acuerdo: hay que gestionar y controlar el riesgo, pero ¿cómo? Porque convivir con situaciones de vulnerabilidades, amenazas o fallas, plantea a las sociedades contemporáneas profundas cuestiones de carácter político y de participación social. Aquí surge el tema de la gobernanza.

Por gobernanza se puede entender la estructura y los procesos para una decisión colectiva, que involucra a actores gubernamentales y no-gubernamentales (Nye and Donahue, 2000). Desde un enfoque institucional, se refiere a las acciones, procesos y mecanismos de participación, por el cual la autoridad es ejercidas y las decisiones son tomadas e implementadas (IRGC, 2006).

De las definiciones se desprende que la gobernanza implica la intervención de aquellos sujetos o entidades que son decisivos, o que de algún modo están involucrados en un tema específico. La participación es multinivel, ya que puede darse el caso de una convocatoria de carácter consultiva a un grupo de expertos en cambio climático, o a empresas que participan en alguna instancia del mercado energético. Pero, también corresponde a los responsables de la administración, la formulación y ejecución de políticas. En todos ellos, el proceso de gobernanza comporta un sentido de responsabilidad e involucramiento de los ciudadanos en la definición de los problemas, así como en el planto de soluciones conjuntas, a pesar de los intereses diversos y de las múltiples perspectivas que puedan tenerse sobre alguna cuestión crítica. Esta dinámica colaborativa requiere de transparencia en la comunicación y de eficacia, en lo que se refiere a la toma de decisiones en la escala y en el momento apropiado (Bevir, 2007).

La "gobernanza de riesgos" adapta los principios y los métodos del mecanismo básico de gobernanza pero, lógicamente, en un entorno de riesgos (Aven and Renn, 2010). Por tal razón, la gobernanza es, también, un proceso de participación y de consulta que sirve para gestionar la complejidad y la incertidumbre (Pierre and Peters, 2005).

En términos institucionales, la gobernanza de riesgos se refiere a la capacidad de las organizaciones y de los ciudadanos en general, para hacer frente a riesgos inevitables. La cuestión es que cuando todo el funcionamiento depende de un sistema complejo de tecnologías una falla puede tener consecuencias catastróficas. Surge, entonces el concepto de gobernanza de riesgos, el cual implica la aplicación de los

principios de una "buena" gobernanza hacia la identificación, evaluación, gestión y comunicación de los riesgos (IRGC, 2010).

Un ejemplo significativo de los nuevos riesgos y de su gestión en un ámbito regional mediante mecanismos de gobernanza, lo reveló la crisis del sistema de interconexión eléctrico europeo en el año 2004, donde a pesar de la pluralidad de actores involucrados, públicos y privados de diferentes países, el conjunto debió actuar de manera coordinada para hacer frente al problema (Gheorghe et al., 2005). Este ejemplo ha mostrado, además, que una adecuada gestión de riesgos: a) posee la ventaja de reducir las externalidades negativas que pueden derivarse potencialmente de las interdependencias negativas o por el contagio de una situación; b) promueve una gestión de la demanda y el ajuste de prioridades en una sociedad; c) reduce los tiempos de restauración del sistema luego de una falla y así, permite que se mantengan los servicios críticos.

Algunas lecciones a tener en cuenta para América Latina

El único futuro posible es que la región asuma una participación activa en la construcción de la sociedad de la información. Así, una nueva visión del desarrollo debe incorporar necesariamente una mejor política de acceso, de inversiones en infraestructuras y de efectivo uso de las nuevas tecnologías (Girard and Perini, 2013).

En la misma línea, el objetivo declarado por los documentos de la CEPAL, en tanto que organismo coordinador de las conferencias ministeriales y reuniones preparatorias frente a las Cumbres mundiales, ha sido desde el documento de Bávaro, "incorporar el proyecto de la sociedad de la información en la agenda del desarrollo" (Cepal, 2003). Paralelamente, se ha reconocido la diversa velocidad de los países en este proceso, junto a una heterogeneidad de respuestas internas- para la incorporación de la SI. Los dos objetivos salientes de la "revolución digital" propuesta en la Declaración de Montevideo y el Plan de trabajo 2013-2015 para la implementación del eLAC2015 son: 1) cerrar brechas en las tecnologías más avanzadas y de impacto masivo 2) acelerar la difusión de tales TIC, lo que implica mejorar el acceso y la apropiación a las mismas (Peres y Hilbert, 2009).

Hay países como Brasil que tienen ya definida una política clara de inserción en el nuevo mundo del conocimiento. Otros, ya tienen inicia-

tivas en estado de avance, como Chile Digital o Argentina Conectada, entre otros. Pero, en la cuestión específica del fortalecimiento de las infraestructuras y del riesgo en las Infraestructuras, aún queda mucho por realizar. Además, una verdadera concepción de la integración regional, no puede dejar de lado la cuestión de las infraestructuras ni la de los riesgos asociados a este proceso.

Algunas ideas que sintetizan los desafíos para América Latina, son:

1. Los diversos temas que surgen de la construcción de la SI van a influir, domésticamente, en la calidad de vida, bienestar y posibilidades de proyección de los ciudadanos; asimismo, influirá sobre la definición de los intereses en las políticas exteriores, en los procesos de cooperación regional y en el comportamiento general de la región.
2. En la SI desarrollarse significa tener más infraestructuras con más tecnologías, pero esto conlleva fragilidad, porque las ventajas poseen una fuerte interconexión con sus potenciales efectos. El desafío de una buena gestión de riesgos descansa, entonces, en el aprovechamiento del beneficio de las TIC, con una estrategia de minimización de las consecuencias negativas asociadas a los riesgos.
3. Es imprescindible la gestión de los riesgos de carácter regional, en especial de lo que poseen un alto nivel de impacto sobre la salud, la seguridad, el medio ambiente, la economía o la sociedad, y que estos sean evaluados mediante mecanismos consultivos con una amplia participación. La dualidad desarrollo-riesgos necesita ser analizada por los diversos públicos interesados (*stakeholders*) e incluida como variable clave por los formuladores de políticas.
4. Las infraestructuras deben ser operadas por empresas (privadas o públicas pero con organización de negocios y búsqueda de rentabilidad. De aquí la necesidad de gobernanza como una herramienta para la gestión integrada cuestiones críticos, donde participan múltiples actores, con intereses y valoraciones diversas.
5. Hay que pensar como objeto de análisis el riesgo específico en las infraestructuras críticas. La seguridad en el abastecimiento del servicio y los impactos que podrían causar una

extensa interrupción de los servicios deberían constituir una prioridad de alto nivel para la legislación, la coordinación de políticas, la planificación y la evaluación de escenarios.

6. Los riesgos globales no están confinados dentro de los límites nacionales, y por lo tanto, no pueden ser gestionados mediante acciones o políticas de un solo sector o gobierno aislado. La gobernanza de riesgos, y de las IC conectadas regionalmente, requiere una especial coordinación entre los países involucrados.

7. Las infraestructuras, en su acelerada evolución, "consumen" productos y servicios, al mismo tiempo que habilitan nuevas capacidades sociales y económicas. Esta situación define el campo de juego del desarrollo: por ejemplo, ¿qué energía se produce y cómo se consume la energía nuclear versus nuevas fuentes?, ¿cuántas empresas pueden generar y distribuir energía? De modo que hay que evaluar los efectos sobre la estructura de trabajo y ampliar los estudios sobre la necesidad / oportunidad de recursos especializados con nuevas habilidades profesionales mediante la ampliación de competencias.

8. Las IC implican una continua formación de las competencias científicas y tecnológicas, a modo de ventaja comparativa dinámica. Pero, puesto que las IC son diseñadas, operadas, mantenidas y utilizadas por personas, las capacidades profesionales estarán determinadas sobre la eficiencia y competencia que puedan obtener en el funcionamiento continuo y estable de las infraestructuras. Los países más desarrollados ya están invirtiendo en la formación de los profesionales y técnicos que tendrán responsabilidad sobre las IC. Y no se trata sólo de ingenieros o técnicos, sino también de economistas, especialistas en leyes, sociólogos, etc.

9. Si bien es verdad que los países se encuentran, por momentos, desgarrados entre distintas demandas y solicitudes, también es cierto que la estructura estatal deberá cumplir nuevas funciones y generar capacidades ampliadas en un escenario cada vez más complejo. Incluso, donde la soberanía no es sólo territorial sino espacial, de allí que surgen innovadores conceptos como "Estado Digital" (Keyworth, 1998) o "Estado Red" (Castellls, 1998).

Como muchos de los riesgos tecnológicos actuales no respetan las fronteras nacionales, surgen también problemas relativos a las políticas de coordinación internacional o regional de los mismos. La gestión de la IIC, y en consecuencia de la SI son por su propia naturaleza realidades a la vez locales, regionales y globales.

Como ejemplo, representantes de los cerca de 80 países se reunieron en San Pablo, Brasil, a fines de abril de 2014 en la "Reunión Global de Múltiples Partes Interesadas sobre el Futuro de la Gobernanza de Internet (NETmundial)". La Declaración Multisectorial emitida recalca la necesidad de contar con más diálogo sobre la gobernanza de Internet para fijar parámetros entre amenazas y derechos para que iniciativas en ciberseguridad deben implicar la colaboración tanto de gobiernos como del sector privado, la sociedad civil, la academia y la comunidad tecnológica (NETMundial, 2014).

En suma, se plantea la importancia de: 1) fundamentar estrategias para la inserción de América Latina en la comunidad internacional denominada SI; 2) planificar un sendero de crecimiento de las IC, teniendo en cuenta riesgos y amenazas potenciales; 3) implementar mecanismos de participación para la gestión de la riesgos, basados en el desarrollo sostenible y la gobernanza; 4) en un plano más operativo, formular las bases para políticas públicas encaminadas a la gestión y regulación del riesgo.

Reflexión final: la gobernanza como estrategia

La SI implica el ingreso a una era signada por la globalización y la complejidad, donde la inestabilidad y la inseguridad no son meramente variables exógenas y circunstanciales, sino rasgos estructurales del sistema social. Es la paradoja del progreso: más desarrollo conlleva una mayor fragilidad.

Las ventajas que trae el uso masivo y ubicuo de las TIC, pueden convertirse al mismo tiempo en amenazas significativas, debido a sus problemas de seguridad, en niveles y extensión que son difíciles de prever, tanto como es arduo predecir la evolución de las tecnologías y sus empleos futuros. Por ello, la confiabilidad de las infraestructuras críticas y la confianza que el ciudadano y la sociedad pueden poner en ellas, están en el centro de la cuestión.

En particular, las vulnerabilidades de las IC pueden ser gestionadas a través de mecanismos y políticas de gobernanza, representando ésta un nuevo tipo de colaboración entre actores públicos y privados en la toma de decisiones colectivas. La elaboración de los libros verdes y libros blancos, son resultados tangibles de estos amplios procesos consultivos y participativos.

Se concluye que los riesgos emergentes en la SI serán en los próximos años cuestiones de máximo interés para el conjunto de los países y que formarán parte ineludible de las agendas. La región latinoamericana, en particular, al igual que los países desarrollados, tendrá que preocuparse de invertir, no sólo en el acrecentamiento de las capacidades en infraestructuras, sino también en su protección, reconociendo su criticidad y su vulnerabilidad.

Referencias

Alexievich, S. (2006). *Voces de Chernóbil*. Crónica del futuro. Madrid, Siglo XXI.

Arpagian, N. (2009). *La Cyberguerre, la guerre numérique a commencé*, Paris, Institut d´estudes et de recherche pur la sécurite des entreprises – Vuibert.

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

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.

Böhme, G. and Nico Stehr (edit.) (1986). *The Knowledge Society. The growing impact of scientific knowledge on social relations*. Dordrech, Reidel-Kluwer.

Canada (2014). *Action Plan for Critical Infrastructure 2014-2017*. Disponible: http://www.publicsafety.gc.ca/cnt/rs-rcs/pblctns/pln-crtcl-nfrstrctr-2014-17/index-eng.aspx

Castells, M. (1999). *La Era de la información*. México D.F., Siglo XXI Editores, 3 vols.

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

Committee on Improving Risk Analysis Approaches (2009). *Advancing Risk Assessment*, Washington D.C., The National Academy Press.

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: 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] (2010). *Emerging risks. Sources, drivers and governance issues*, Geneva, Revised edition.

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

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

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.

NETmundial (2014). "Multistakeholder Statement" (April, 24th, 2014). Disponible en: http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

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.

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

Ortiz, J. (1999). "La Era de la Información Glocal", *Revista de la Escuela Superior de Guerra del Ejército Argentino*, N° 534 (julio-septiembre), p.35-49.

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.

Palma, R., y G. Masera (2014). "Escenarios energéticos. Aplicación del enfoque PESTEL". Mendoza, documento presentado en ECEFI 2014-UTN), *forthcoming*.

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.

Rennstich, J. K. (2008). *The Making of a Digital World*. New York, Palgrave Macmillan.

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

Thompson, P. (1990): "Risk Objectivism and Risk Subjectivism: When Are Risks Real?", *Risk: Health, Safety & Environment*, n°1: 3, HeinOnline.

Webster, F. (2002). "The information Society Revisited", in L. Lievrouw and S. Livingstone (Edit.) *Hand Book 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. First edition 1995.