Bijker, Wiebe E.

La vulnerabilidad de la cultura tecnológica

La vulnerabilidad de la cultura tecnológica*

WIEBE E. BIJKER**

Resumen

Los ataques sobre Nueva York y Washington del 11 de septiembre de 2001, como otros ataques posteriores, han demostrado cuán vulnerables son nuestras sociedades modernas. Estos eventos quebrantaron los sentimientos más básicos de seguridad de mucha gente. Aún así, el 11 de septiembre probablemente no haya cambiado radicalmente la visión de los académicos en ciencia, tecnología y sociedad (CTS). El autor argumenta que vale la pena investigar la vulnerabilidad de la cultura tecnológica, y que esto puede hacerse fructíferamente desde una perspectiva CTS. En el artículo se sugiere que la vulnerabilidad no debe ser considerada como algo puramente negativo. Por el contrario, vivir en una cultura tecnológica implica inevitablemente vivir en un mundo vulnerable, y la vulnerabilidad no es solamente una característica inevitable, es incluso un valor importante de nuestra cultura tecnológica como prerrequisito para la búsqueda de la innovación.

PALABRAS CLAVE: RIESGO – VULNERABILIDAD – CULTURA TECNOLÓGICA

Los ataques del 11 de septiembre de 2001 (9/11) a Nueva York y Washington, así como otros ataques que se han producido desde entonces, han demostrado cuán vulnerables son nuestras modernas sociedades.[1] Estos eventos hicieron añicos muchos sentimientos de seguridad y salvaguarda básicos, aunque sin embargo el 9/11 probablemente no haya cam-

* Esta es una versión preliminar del texto publicado como Bijker, W. (2006), "The Vulnerability of Technological Culture", en Nowotny, H. (ed.), *Cultures of Technology and the Quest for Innovation*, Nueva York, Berghahn Books, pp. 52-69. Traducción de Alfonso Buch.

** Profesor y decano del Departamento de Ciencias Sociales y Tecnología, en la Facultad de Artes y Cultura de la Universidad de Maastricht, Holanda. E-mail: < W.Bijker@TSS.unimaas.nl>

[1] Este artículo es el resultado de numerosas discusiones con mucha gente. Quiero agradecer a Wes Shrum, Rosalind Williams, Steve Rayner y Steve Woolgar. También me beneficié mucho de los comentarios de los participantes de la reunión de trabajo de marzo de 2002 en el MIT (véase nota 2); la conferencia "Cultures of Technology and the Quest for Innovation" en Essen en abril de 2003; el coloquio sobre CTS en Maastricht en mayo de 2003; y un seminario en la Said Business School, Universidad de Oxford en junio de 2003. Un agradecimiento especial a Karin Bijsterveld, Helga Nowotny, Ger Wackers y Rein de Wilde por la discusión de un borrador previo.

biado radicalmente la mirada de los especialistas en los estudios sobre ciencia, tecnología y sociedad (CTS). El trabajo en torno a este capítulo comenzó en respuesta al 9/11, cuando muchos historiadores y sociólogos de la ciencia y la tecnología se preguntaron de qué modo su investigación podía ser relevante para la comprensión de esos eventos.[2] Considero que es valioso investigar la vulnerabilidad de la cultura tecnológica, y qué puede hacerse fructíferamente desde la perspectiva de los estudios CTS, sin embargo, mi argumento principal es otro. Quiero sugerir que la vulnerabilidad no debe tomarse como algo puramente negativo. Argumentaré que vivir en una cultura tecnológica implica inevitablemente vivir en un mundo vulnerable. Y la vulnerabilidad no solo es una característica inevitable, sino que incluso también es un importante recurso de nuestra cultura tecnológica como condición previa para vivir en la búsqueda de la innovación. Para vivir en una cultura abierta, cambiante e innovativa debemos pagar el precio de la vulnerabilidad.

La vulnerabilidad es una cuestión central cuando pensamos sobre la innovación. El reconocimiento realizado por Joseph Schumpeter de que la inestabilidad fundamental del capitalismo presenta una posibilidad siempre presente de aprovechar las innovaciones por parte de los empresarios, puede interpretarse como una formulación temprana de una relación positiva. En tanto resultado inevitable de la inestabilidad y del desarrollo dinámico que Schumpeter identificó como condición previa para la innovación (Schumpeter, 1939), la vulnerabilidad parece ser una condición *sine qua non*. La relación puede plantearse a la inversa; la innovación construye vulnerabilidad. Las leyes de patentes, por ejemplo, son un modo de arreglárselas con la vulnerabilidad financiera que resulta de las grandes inversiones necesarias para la innovación.

En este artículo quiero explorar la vulnerabilidad de la cultura tecnológica: una vulnerabilidad que es al mismo tiempo una consecuencia inevitable y un prerrequisito necesario de la sociedad tecnológica avanzada en la cual vivimos. Para hacer esto voy a especificar primero qué significa investigar la *cultura* tecnológica más allá del análisis de los *sistemas* tecnológicos y la *sociedad* de alta tecnología, y luego continuaré con un análisis del concepto de vulnerabilidad aplicado a los sistemas, la sociedad y la cultura, respectivamente.

[2] Un primer repertorio y discusión acerca de las implicaciones que el 9/11 puede tener para el estudio de la tecnología en la sociedad fueron los resultados de una reunión de trabajo llevada a cabo en marzo de 2002, en el marco del programa CTS del MIT (Levin y Williams, 2003). Para posicionar esta investigación sobre vulnerabilidad en el trabajo actual en CTS, daré más referencias de lo que sería necesario para la cuestión de la vulnerabilidad en sí misma.

ESTUDIANDO LA CULTURA TECNOLÓGICA

Tal como lo observa Helga Nowotny (2003), "aproximarse a la tecnología bajo una perspectiva cultural es [...] tan autoevidente como altamente exigente". Una aproximación de este tipo es autoevidente porque "la tecnología es percibida como la práctica cultural desarrollada por la especie humana que mayores consecuencias posee"; y es exigente porque "los riesgos asociados con las tecnologías han revelado ser ellos mismos fenómenos culturales también". Por consiguiente, para analizar los diversos tipos de vulnerabilidad de los sistemas tecnológicos y de las sociedades es necesario utilizar una perspectiva cultural, es necesario analizar la cultura tecnológica.

Este foco en la cultura tecnológica es parte de una tendencia más general en CTS. En los años 1970 y 1980 el foco estaba en estudios de caso de controversias científicas y en artefactos y sistemas tecnológicos. En la década de 1990 esta agenda se amplió incluyendo también cuestiones sociales, políticas y culturales de relevancia social (Edwards, 1996; Hecht, 1998; Browker y Star, 1999). La base empírica fue ampliada en consonancia; la atención a la ciencia fue extendida también a una variedad de sistemas de creencias tales como el conocimiento indígena (Watson-Verran y Turnbull, 1995; Verran, 2001), y el conocimiento desarrollado por grupos de pacientes (Epstein, 1996). Asimismo, los estudios sobre tecnologías incluyeron a las tecnologías sociales y a los usuarios de las tecnologías (Oudshoorn y Pinch, 2003). La agenda de investigación de los estudios CTS abarca ahora también cuestiones tales como la democratización, la pericia (científica), política genómica, y la relación entre desarrollo económico y conocimiento tecnológico (Gottweis, 1998; Callon *et al.*, 2001; Bal *et al.*, 2002; De Wilde *et al.*, 2002; Mokyr, 2002). En otras palabras, los desarrollos en la última década han mostrado un cambio del estudio de las culturas (locales) de la ciencia y la tecnología al estudio de la cultura tecnológica ampliada.

¿Por qué usar la expresión "cultura tecnológica"? Una razón es para destacar la omnipresencia de la ciencia y la tecnología en las sociedades modernas altamente desarrolladas. Tal como lo resumimos con John Law en 1992:

> Todas las relaciones deben ser vistas como sociales y técnicas [...] Relaciones puramente sociales pueden encontrarse solo en la imaginación de los sociólogos, entre los babuinos o, posiblemente, solo posiblemente, en las playas nudistas; y relaciones puramente técnicas pueden encontrarse solo en las extensiones salvajes de la ciencia ficción (Law y Bijker, 1992: 290).

En la conceptualización de la sociedad como una combinación de sistemas meramente sociales y sistemas tecnológicos no se reconoce adecuadamente esta omnipresencia. En cambio, tomar a la "cultura tecnológica" como el foco clave de la investigación ayuda a reconocer "la asunción básica subyacente de que las sociedades modernas son formadas predominantemente por el conocimiento y la tecnología".[3] Estudiar la cultura tecnológica entonces significa estudiar tecnologías y sociedades desde una perspectiva cultural. Un foco en la cultura tecnológica destaca cómo la interacción social está mediada por tecnologías y cómo las tecnologías pueden funcionar solo cuando están embebidas por instituciones sociales.

De tal modo este uso de la expresión "cultura tecnológica" es más amplio y más ambicioso que aquel en que es usado en el campo de la percepción pública de la ciencia; en ese caso es sinónimo de "alfabetización técnológica" y muchas veces está vinculado con desarrollo económico e innovación.[4] El término "cultura tecnológica" en su sentido más amplio está en línea con el movimiento de Manuel Castells de extender el análisis de la sociedad en red a un análisis sobre la identidad, la democracia, el poder y las relaciones internacionales (Castells, 1997, 2000a, 2000b). Está igualmente en línea con trabajos recientes en filosofía que reconocen "que los rasgos característicos de nuestra cultura son pervasivos e irrevocablemente tecnológicos", y que todos los debates públicos actuales "involucran percepciones de la tecnología en su sentido más amplio y comprensivo, es decir, *la tecnología como nuestra cultura*".[5]

Voy ahora a revisar con más detalle qué significa estudiar la vulnerabilidad de los sistemas tecnológicos y las sociedades de alta tecnología desde una perspectiva cultural, y después resumiré estos hallazgos discutiendo la vulnerabilidad de la cultura tecnológica.

SISTEMAS VULNERABLES

Los sistemas tecnológicos pueden ser vulnerables, lo que queda suficientemente claro a partir de una larga lista de accidentes y de tratados especializados anexos (Schlager, 1994). Charles Perrow ya planteó en 1984 que en las sociedades modernas, con sus sistemas tecnológicos grandes, complejos y estrechamente interconectados, los accidentes son "normales" (Perrow, 1999). La

[3] Esta es la caracterización que Michael Guggenheim y Helga Nowotny dan acerca de lo que distingue los ECT de otras ciencias sociales (Guggenheim y Nowotny, 2003: 241).

[4] Véase por ejemplo Godin y Gingras (2000). Usé por primera vez la expresión "cultura tecnológica" en mi lección inaugural: Bijker (1995a), en holandés. Véase también Bijker (1995b).

[5] Itálicas en el original: Hickman (2001: 1-3). Véase también Keulartz *et al.* (2002, 2004).

literatura reciente de los estudios CTS abarca, por ejemplo, el desastre del Challenger (Vaughan, 1996), la explosión de la planta química de Bhopal (Fortun, 2001), accidentes de aviación (La Porte, 1988; Rochlin, 1991; Snook, 2000; Wackers y Kørte, 2003), y accidentes nucleares (Rochlin, 1994).

El significado común de vulnerable es "susceptible de ser lastimado o herido" y muchas veces se aplica a ecosistemas o seres vivos. Connotaciones asociadas son: indefenso, no preparado, débil y desnudo. Vulnerable, entonces, parece describir una característica intrínseca de un ser o un sistema, de manera bastante independiente al contexto concreto del sistema. Es más provechoso sin embargo analizar la vulnerabilidad como un concepto relacional. Escribiendo acerca de peligros naturales Piers Blaikie y sus coautores ofrecen una definición relacional y activa de la vulnerabilidad: la "capacidad [reducida] para anticipar, tratar, resistir, y recuperarse del impacto de un peligro natural" (Blaikie *et al.,* 1994: 9). Algunas veces, asociado con este significado activo, también se da una connotación más positiva de ser vulnerable: bajar tus defensas, exponer tus puntos débiles, mostrar tus talones de Aquiles –lo cual puede ser una expresión de fuerza y superioridad más que de debilidad. En esta sección voy a investigar estos aspectos –relacionales, activos, y parcialmente positivos– desarrollando más el concepto de vulnerabilidad en conexión a los sistemas técnicos. Lo haré en cuatro pasos.

Al analizar la vulnerabilidad de los sistemas tecnológicos Ger Wackers y Jens Kørte desconstruyen esta capacidad reducida para anticipar, tratar, resistir y recuperarse de las amenazas y la traducen en una capacidad reducida para mantener la integridad funcional. Sin esta integridad funcional, los sistemas dejan de operar; para los seres vivientes, la pérdida de integridad funcional significa la muerte (Wackers y Kørte, 2003). Esto apunta a mi primer paso hacia la especificación de la vulnerabilidad. Con este concepto de (pérdida de) integración funcional, Wackers y Kørte analizan la vulnerabilidad de un sistema de transporte de helicópteros de apoyo a explotaciones petrolíferas mar adentro. Muestran cómo el sistema de helicópteros *derivaba* (i.e. cambiaba imperceptiblemente) hacia un estado más vulnerable en el cual varios elementos funcionaban en un nivel subóptimo y en el cual las adaptaciones –aparentemente prácticas– de los protocolos prescritos resultaban en un incremento en la vulnerabilidad del sistema.

El concepto "deriva" ha sido usado por una variedad de autores, pero Wackers y Kørte recurren en particular al análisis de Scott Snook acerca del derribo por parte de dos cazas norteamericanos, de dos helicópteros de que transportaban oficiales de las fuerzas de paz de las Naciones Unidas en el norte de Irak (Snook, 2000). Snook describe cómo una "deriva práctica" de adaptaciones y procedimientos locales condujo a una separación creciente y

constante entre las normas de seguridad y las operaciones prácticas de cazas, helicópteros y controladores Awacs.* Individualmente, estas adaptaciones carecían de consecuencias, pero en un largo período esta deriva práctica había resultado en un sistema vulnerable –el sistema había perdido parte de su funcionalidad debido a que varios subsistemas no colaboraban ni se integraban de acuerdo a lo previsto.

¿Qué podemos significar exactamente con el término "sistema vulnerable"? El análisis de Charles Perrow acerca de los grandes sistemas (técnicos) es el punto de partida clásico para responder esta pregunta. El diagnóstico de Perrow es que los grandes sistemas técnicos son más riesgosos, y tienden a dirigirse hacia accidentes más catastróficos cuando son más complejos y más estrechamente interconectados. Los sistemas complejos –en contraste con los sistemas lineales– poseen muchos subsistemas interconectados, con muchos bucles de realimentación, y controles interactivos múltiples. Ejemplos de ellos son las universidades y las plantas nucleares. Los sistemas estrechamente interconectados –en contraste con los débilmente interconectados– no permiten retrasos en el procesamiento, siguen una secuencia invariante de pasos, tienen pocas pausas en los suministros y el personal, y pocos elementos moderadores y/o redundantes integrados. Ejemplos de ellos son las represas hidroeléctricas y las plantas nucleares.

Los sistemas aéreos y las plantas nucleares son sistemas complejos *y* estrechamente interconectados. Utilizando el análisis de Perrow es posible ahora dar un segundo paso hacia la especificación de la vulnerabilidad de los sistemas. Un sistema complejo estrechamente asociado es más vulnerable de dos modos: 1) tiene más riesgo de falla, en el sentido de Perrow, debido a errores de algún componente interno y 2) es menos capaz de anticipar, manejar y recuperarse del impacto de perturbaciones externas que no se ajustan a sus líneas de reacción preconcebidas. En otras palabras, un sistema débilmente interconectado es menos vulnerable en ambos sentidos debido a que hay menos chances de que proliferen los errores internos a través del sistema, y porque hay más oportunidades para reaccionar frente a perturbaciones externas (bajo la forma de disponibilidad de tiempo, de elementos moderadores y/o redundantes). Además, un sistema lineal puede ser protegido más fácilmente –y por lo tanto puede hacerse menos vulnerable– porque típicamente, está espacialmente segregado, permite fáciles sustituciones de subsistemas y componentes, tiene controles sencillos y pocos bucles de realimentación, y a menudo es mejor entendido.

* Acrónimo de *Airborne Warning and Control System*, un sistema de control y alerta basado en el empleo de grandes radares aerotransportados [N. del T.].

El trabajo de Perow, Snook, Wackers y Kørte muestra cuán crucial es analizar estos eventos como una combinación de individuos, grupos y niveles de sistemas. Diane Vaughan añade a estas perspectivas la cultura grupal y la cultura organizacional –y este es mi tercer paso. Ella reconoce el desastre del Challenger como un accidente normal, pero "este caso extiende la noción de sistema de Perrow hasta incluir aspectos tanto del ambiente como de la organización que afectan el proceso de evaluación del riesgo así como la toma de decisiones". La interpretación de los expertos técnicos "sobre las señales, está sujeto a errores formados por un sistema aún más amplio que incluye historia, competencia, escasez, procedimientos burocráticos, poder, reglas y normas, jerarquía, cultura y patrones de información" (Vaughan, 1996: 415). En el epílogo a la edición de 1999 de su libro de 1984, Perrow critica el foco puesto por Vaughan en la cultura y la seguridad del grupo de trabajo porque ella "[se] pregunta cómo podemos hacer que los sistemas riesgosos con potencial catastrófico sean más seguros, una pregunta que da por sentado que deben ser más calientes, más grandes, más tóxicos, y harán más demandas a los miembros". Además Perrow quiere plantear la cuestión del poder y "el papel de las presiones productivas en sistemas crecientemente privatizados y desregulados que pueden evadir el escrutinio y la responsabilidad" (Perrow, 1999: 379). Estoy de acuerdo con la disposición de Perrow para poner en primer plano la elección política entre tecnologías específicas y sobre formas de organizar la sociedad, pero creo que pierde de vista el punto clave del análisis cultural de Vaughan.

Considero que en su análisis, Vaughan no desestima la importancia de las cuestiones de la política y el poder, pero arroja sobre ellos una luz diferente.

Esto formará mi cuarto paso en el desarrollo del concepto de vulnerabilidad de los sistemas: Diane Vaughan vincula su análisis cultural explícitamente con la noción de flexibilidad interpretativa del constructivismo social (Bijker, 1995b):

> La ambigüedad del oficio de ingeniero se complica con la "flexibilidad interpretativa". Varias pruebas del mismo fenómeno no solo producen diferentes resultados sino que los hallazgos de una sola prueba están abiertos a más de una interpretación (Vaughan, 1996: 202).

Y también señala:

> […] incluso los mismos resultados pueden interpretarse de modos diferentes. Algunas veces los desacuerdos entre las dos comunidades eran difíciles de resolver debido a que, como lo indicó un experimentado representante de Marshall S & E, los ingenieros de las empresas contratistas tendían a ser

> "defensivos en lo que hace a sus diseños" dado que creían en sus propios métodos y sus análisis (Vaughan, 1996: 87).

Esta percepción implica que la vulnerabilidad de los sistemas no puede caracterizarse en términos objetivos, independientes al contexto, La vulnerabilidad, quisiera argumentar, es construida socialmente tanto como lo son los hechos y los artefactos (Pinch y Bijker, 1984).

Para elaborar este argumento es útil considerar primero el concepto relacionado de *riesgo*. La vulnerabilidad de los sistemas, y en particular la vulnerabilidad debida a posibles errores internos y fracasos, puede ser descripta hasta cierto punto en términos de riesgos. El Consejo de Salud de los Países Bajos define riesgo como "la posibilidad (con algún grado de probabilidad) de que ocurra un perjuicio (con un carácter y tamaño específicos) a la salud, la ecología o los bienes" (Gezondheidsraad, 1995: 14). Esta es una definición deliberadamente amplia, que puede incluir una variedad de formas de perjuicio: variando por ejemplo en carácter, magnitud, oportunidad y posibilidad de recuperación. Es más amplia que la definición que forma la base del análisis probabilístico de riesgo; la probabilidad de un evento (perjudicial) multiplicado por su magnitud. La amplitud de la definición del Consejo de Salud implica una forma de análisis de riesgo y gerenciamiento que reconoce que "el riesgo es más que un número" –el título de otro informe del Consejo de Salud (Gezondheidsraad, 1996).

En este último informe se reconoce que los riesgos son la consecuencia de la acción humana; sea si consideramos la producción de energía nuclear, las plantas químicas, los viajes aéreos, vivir bajo el nivel del mar o fumar, tales acciones humanas siempre apuntan a algún tipo de ganancia o beneficio. Por lo tanto es necesario evaluar riesgos y beneficios dentro de un marco de trabajo: los riesgos no pueden ser evaluados sin evaluar también los efectos positivos de las acciones que los generan. Además, el Consejo de Salud concluye que los problemas de riesgo pueden variar fundamentalmente en función de la extensión del riesgo en el tiempo; su extensión en el espacio; la incertidumbre acerca de su extensión, carácter y magnitud; y la relevancia social de la acción inductora del riesgo. Todas estas consideraciones llevan a la conclusión de que la distinción entre riesgo objetivo y percepción de riesgo empleada a menudo, no se sostiene. Los riesgos no pueden ser conceptualizados como fenómenos objetivos, cuantificables, independientes del contexto, y no tiene sentido tampoco hablar de la percepción de tales riesgos objetivos (Van Asselt, 2000).

Ahora puedo especificar la relación entre vulnerabilidad y riesgo. Vulnerabilidad refiere a una *condición* de un sistema –a su capacidad para

anticiparse, resistir, tratar y posiblemente recuperarse de los eventos que pueden reducir la integridad funcional de los sistemas. Por su parte, riesgo es una noción orientada hacia el resultado, conceptualiza los *efectos* de un evento perjudicial posible. La vulnerabilidad, por sí misma, no está relacionada a ningún otro resultado distinto que la avería del sistema en sí mismo. Un sistema vulnerable puede producir ciertos riesgos cuando, dependiendo de las circunstancias, puede producir daño. Recíprocamente, un análisis de riesgo puede ser útil en la evaluación de la vulnerabilidad de un sistema: analizar las posibilidades (y el daño resultante) de la falla de un subsistema o componente puede ayudar a intentar comprender al menos los aspectos técnicos de la vulnerabilidad de un sistema.

Déjesenos terminar ahora el cuarto paso –el giro constructivista– en el desarrollo del concepto de vulnerabilidad. El primer movimiento fue el reconocimiento de Vaughan de la flexibilidad interpretativa de las afirmaciones acerca de las características y el rendimiento de un sistema. El segundo movimiento fue reconocer que incluso los riesgos eran "más que números" y que en verdad eran dependientes del contexto y de la cultura. Para completar este giro constructivista con un tercer movimiento tomaré elementos del artículo de John Law sobre el desastre ferroviario London Ladbroke Grove (Law, 2003). En este trágico accidente, en el que murieron 31 personas y resultaron heridas 414, un tren diesel con tres vagones chocó con un tren de alta velocidad en Ladbroke Grove, a dos millas de la estación Paddington el 5 de octubre de 1999. Usando un análisis del tipo actor-red Law produce una descripción detallada del sistema relevante, incluyendo las unidades ferroviarias, las señalizaciones, los programas de capacitación de los conductores, el gerenciamiento industrial, y las regulaciones y tecnologías de seguridad. El análisis de Law nos muestra cómo todos los elementos de la red –tanto las personas como las tecnologías– fueron adaptados hacia el mantenimiento y el mejoramiento de la seguridad. Pero también muestra cómo pequeños cambios en los arreglos estándar pueden haber "derivado" de manera acumulativa hacia este desastre. Hay una diferencia crucial sin embargo entre el manejo que hace Snook del concepto de deriva práctica y la conclusión de Law acerca del papel de los pequeños desórdenes que condujeron al desastre de Ladbroke Grove.

Law destaca que "el desorden parcial de estos arreglos no muy coherentes funciona bien en la mayoría, si no en todas, las circunstancias. [...] Por cada caso de un Ladbroke Grove hay un sin fin de 'quiebres de sistemas' que no tienen consecuencias serias". Muestra asimismo con un detallado análisis del uso del *Driver Reminder Appliance* (DRA) en el tren diesel (que no puedo reproducir aquí) que la misma medida que fortalece el sistema y lo hace

menos vulnerable bajo un conjunto de circunstancias hace exactamente lo opuesto bajo otras circunstancias y aumenta la vulnerabilidad del sistema. De tal modo estas medidas, estos dispositivos técnicos, y estas regulaciones muestran flexibilidad interpretativa: bajo una condición mejoran la seguridad y bajo otras incrementan la vulnerabilidad.

De un modo más crucial para mi concepción constructivista de la vulnerabilidad, Law argumenta que "hay interminables fallas en los sistemas que ayudan a mantener las ruedas girando". El argumento de Law aquí es un argumento acerca de la imperfección: acerca de su carácter inevitable, y acerca de las ventajas de practicar la imperfección. Este es el modo en que los sistemas complejos se han desarrollado a lo largo del tiempo: se han desarrollado prácticas y rutinas en contextos de seguridad crítica porque demostraban ser factibles y de tal modo producían un sistema relativamente estable e invulnerable. Y algunas de estas prácticas son incoherentes, indisciplinadas, contrarias a las regulaciones de seguridad estrechamente interpretadas. Tales prácticas indisciplinadas son el lubricante que mantiene en funcionamiento un sistema, que hace menos vulnerable un sistema tratando mejor los potenciales peligros. La conclusión, entonces, puede ser solo que la vulnerabilidad está construida socialmente: el mismo sistema puede juzgarse relativamente invulnerable (cuando se interpreta al comportamiento indisciplinado como que la gente está asumiendo su responsabilidad, utilizando su experiencia, improvisando para acomodarse a condiciones cambiantes) o estimado vulnerable (cuando se define dicha indisciplina como una violación de las reglamentaciones que crea situaciones de riesgo).

Déjeseme resumir mi análisis cultural de la vulnerabilidad de los sistemas tecnológicos. La vulnerabilidad de un sistema tecnológico refiere a la debilidad de la capacidad de ese sistema para mantener su integridad funcional. La vulnerabilidad del sistema está vinculada al funcionamiento de los subsistemas, los componentes de los sistemas, y a las rutinas y las prácticas laborales. Por lo tanto el análisis de riesgo en el nivel de los componentes puede ser útil para evaluar la vulnerabilidad de un sistema. La deriva práctica puede conducir gradualmente a un sistema hacia estados más vulnerables, sin que los practicantes lo noten en ese momento. La vulnerabilidad es un concepto constructivista en el sentido de que no describe independencia respecto al contexto y una cualidad intrínseca en el sistema. Tal como la sociología del conocimiento ha mostrado para los enunciados científicos, la vulnerabilidad será puesta en cuestión cuando se encuentre en el centro del debate, de la controversia o de la investigación. Esto no quiere decir que todo está meramente "en el ojo de quien lo mira" o que no hay base real en la vulnerabilidad. Déjeseme adaptar la siguiente metáfora, utilizada por Harry Collins para

ilustrar la naturaleza construida del conocimiento científico: la vulnerabilidad y el sistema son como el mapa y el paisaje –la vulnerabilidad se relaciona con la realidad del sistema, pero no está determinada totalmente por él.[6]

Sociedades vulnerables

Los sistemas técnicos funcionan en sociedades. Las sociedades modernas, altamente tecnológicas, están en verdad construidas sobre, con, en torno a, y en sistemas tecnológicos. Cualquier falla en esos sistemas tecnológicos, por tanto, afectará directamente a la sociedad. Sistemas técnicos vulnerables conducen a sociedades técnicas vulnerables. El concepto de vulnerabilidad, tal como está desarrollado en la sección precedente, es totalmente aplicable a las sociedades –de su foco en la integridad funcional a su naturaleza construida.

Cuando describimos nuestras sociedades como vulnerables a un ataque terrorista queremos decir que hay una posibilidad que un ataque de ese tipo haga que dejen de funcionar instituciones claves de la sociedad y que se desintegre la estructura de la sociedad. En este diagnóstico acerca de la vulnerabilidad, la tecnología juega un papel clave. Las sociedades occidentales son más vulnerables *debido* a que son sociedades de alta tecnología. Es justamente debido a que instituciones clave tales como la distribución de energía, las comunicaciones, el transporte y el comercio son tan complejas y están tan estrechamente interconectadas, que una sociedad de alta tecnología construida en torno a estas instituciones es tan vulnerable. La mayoría de estos sistemas tecnológicos y de estas instituciones sociales han existido de algún modo desde ya largo tiempo, pero su carácter complejo y asociado es nuevo. Tal como lo observa Perrow:

> La nave de Odiseo no contaminaba la costa del Mediterráneo ni podía destruir mucho de la ciudad de Texas; los bombarderos de la Segunda Guerra Mundial no podían chocar en un edificio que contuviera armas nucleares, [...] las plantas químicas no eran tan grandes, no estaban tan cerca de las comunidades o procesaban químicos tan explosivos y tóxicos; las líneas aéreas no eran tan grandes, tan numerosas o tan cercanas a comunidades tan grandes; y solo recientemente se ha conocido en casi todas las zonas densamente pobladas de nuestro país el riesgo de radiación por un accidente en una planta nuclear (Perrow, 1999: 307).

[6] Una consideración constructivista similar de la vulnerabilidad es discutida por Kristin Shrader-Frechette (1991). En estas discusiones sobre el riesgo, sin embargo, se crea un contraste en la evaluación de riesgo entre el "campo constructivista" y el "campo realista". No estoy de acuerdo con esta distinción porque la sugerencia subyacente es que los datos científicos son más reales que otro tipo de información (Klinke y Renn, 2002).

Los daños pueden venir de adentro o de afuera de los sistemas tecnológicos; los daños pueden provenir bajo la forma de errores técnicos y accidentes, o bajo la forma de disrupciones sociales –pero en todos los casos el carácter complejo y estrechamente asociado de las instituciones de alta tecnología incrementa potencialmente el efecto devastador del daño.

Pero también es cierto lo contrario. Las sociedades occidentales nunca han estado tan bien defendidas contra desastres naturales como con los sistemas actuales de diques y los edificios a prueba de terremotos. La tecnología de vigilancia, inteligencia, los sistemas de información y las tecnologías biométricas para la identificación personal defiende a los Estados Unidos contra intrusos. Las tecnologías médicas modernas han acrecentado la salud pública a niveles sin precedentes. Nuestras sociedades occidentales son menos vulnerables debido a los sistemas tecnológicos que son empleados. Este diagnóstico al parecer contradictorio –que la tecnología hace a las sociedades modernas más vulnerables, mientras que al mismo tiempo las hace más seguras– sería por supuesto solo un problema para un concepto esencialista de vulnerabilidad: una sociedad es "realmente" vulnerable en algunos grados. El concepto constructivista de vulnerabilidad que he propuesto en el apartado precedente reconoce que bajo ciertas condiciones, ciertos actores, con ciertos objetivos pueden construir una sociedad vulnerable, en tanto que puede plantearse que la misma sociedad es relativamente invulnerable en otro contexto o bajo otra perspectiva.

Algunos de los trabajos recientes sobre vulnerabilidad, muchas veces espoleados por los ataques terroristas, reflejan este carácter dual de las sociedades tecnológicas. Más allá de la atención reciente puesta en ayudar a que los ciudadanos se preparen a sí mismos contra ataques terroristas, muchas de las discusiones y actividades relacionadas con la vulnerabilidad han estado focalizadas en asuntos de infraestructura (Blaikie *et al.*, 1994; Branscomb, 2002). Muchas veces esto ocurrió en el contexto de desastres naturales tales como inundaciones y terremotos. En los últimos tiempos, la infraestructura de internet ha recibido una atención creciente y en diferentes sentidos: como una infraestructura potencialmente vulnerable de la sociedad moderna, como una infraestructura que puede fortalecer la capacidad de la sociedad para reaccionar a las amenazas, e incluso como una infraestructura que puede ser transformada en un arma para atacar a la sociedad.[7]

[7] La literatura sobre la vulnerabilidad de las computadoras y de internet es enorme y aún en crecimiento, incluyendo revistas completas y bases de datos *on-line*. El uso de internet y las computadoras para la guerra y el terrorismo ha sido denominada "cyberwar" –guerra cibernética– o "netwar" –guerra red– (Arquilla, 2001).

Conectar la noción de vulnerabilidad con la supervivencia de las naciones es por supuesto algo que ha sido hecho frecuentemente desde el 9/11, y especialmente en los Estados Unidos. Significativamente la palabra "vulnerable" casi nunca es usada en los documentos y los sitios de internet del nuevo Departamento de Seguridad Nacional de los Estados Unidos, si bien se podría decir que es el concepto más importante que se encuentra detrás de las acciones y políticas de este ministerio. Se cita la vulnerabilidad a "amenazas biológicas, químicas y radiactivas, y a explosiones convencionales y nucleares" como la principal razón para "estar listo", "estar informado", "hacer un plan", y "hacer un equipo de suministros de emergencia".[8] Por supuesto, entre especialistas (pero ahora me estoy refiriendo a especialistas militares y en armamento más que a especialistas en los estudios CTS) hace ya largo tiempo que se ha reconocido "la vulnerabilidad de los Estados Unidos a ataques realizados por terroristas internacionales o grupos domésticos o por tales grupos con vínculos domésticos-internacionales" (Sloan, 1995: 5). El énfasis era sobre armas nucleares, químicas y biológicas:

> La proliferación de las armas nucleares y sus tecnologías asociadas, así como la difusión del conocimiento necesario para fabricar armas químicas y biológicas, hace surgir el temible espectro de la destrucción en masa de un modo tal que el uso del ántrax como un modo de difundir tanto la enfermedad como el pánico palidece hasta la insignificancia. La temible verdad es que Estados Unidos es demasiado vulnerable a este tipo de ataque [...] Los blancos altamente simbólicos tales como los edificios gubernamentales y las sedes de corporaciones serán más vulnerables a los ataques (Sloan, 1995: 7).

Estos relatos, comentarios y políticas ejemplifican la naturaleza construida de la vulnerabilidad: crean una forma particular de vulnerabilidad, vinculada con una identidad particular de la sociedad norteamericana. Existen otras sociedades americanas, y tal como mostraré más adelante, de acuerdo con ello pueden construirse otros relatos sobre la vulnerabilidad y la resiliencia.

De tal modo, el concepto de vulnerabilidad tal como lo he presentado antes, también es aplicable a las sociedades; sin embargo, puede necesitar cierta ampliación. Hay algunas cuestiones que juegan un papel cuando se discute la vulnerabilidad de una sociedad, que no son preponderantes cuando se discuten sistemas tecnológicos. El Consejo de Salud de los Países Bajos explícitamente concluye a partir de su diagnóstico que el riesgo es más que un número:

[8] Véase el sitio de internet del Departamento de Seguridad Nacional de los Estados Unidos: }<http://www.ready.gov/>, visitado el 12/01/2004.

> Los problemas sobre la gestión del riesgo son problemas acerca de la configuración de la sociedad. Las opiniones sobre la vulnerabilidad de la naturaleza, acerca del cuidado de las generaciones futuras, y acerca de la libertad para actuar –todas ellas forman las respuestas a estos problemas (Gezondheidsraad, 1996: 20).

Estas son cuestiones que se relacionan con los valores centrales de una sociedad. Perrow también nota la dificultad de manejar estos problemas con los modelos matemáticos que dominan el campo del análisis probabilístico del riesgo:

> [Este] es un campo estrecho, atenazado por la monetarización de los bienes sociales. Todo puede ser comprado; si no puede ser comprado no entra en los sofisticados cálculos. Una vida vale aproximadamente 300 mil dólares [...]; menos si usted tiene más de sesenta años, menos incluso si además está debilitado (Perrow, 1999: 308).

Debe añadirse un segundo elemento para completar esta sección sobre las sociedades vulnerables, que involucra el papel de la ciencia. En su análisis acerca de la sociedad moderna como una "sociedad de riesgo", Ulrich Beck identifica el nuevo papel crucial que juega la ciencia en la vulnerabilidad de las modernas sociedades de alta tecnología (si bien él no usa la palabra "vulnerable"):

> Si estuvimos previamente preocupados por peligros causados *externamente* (por los dioses o la naturaleza), la nueva cualidad histórica de los riesgos de hoy derivan de las *decisiones internas*. Dependen de una *construcción científica y social* simultánea. La ciencia es *una de sus causas, el medio para definirlos y la fuente de las soluciones* a los riesgos (Beck, 1992: 155, itálicas en el original).

El análisis de Beck le da a la concepción de vulnerabilidad que desarrollé hasta el momento un importante giro reflexivo. La vulnerabilidad de la sociedad no es, como consideraría Perrow, el mero resultado del crecimiento en número, tamaño, complejidad y en la naturaleza estrechamente asociada de los sistemas tecnológicos. Beck concibe los riesgos, los accidentes y –yo añadiría– la vulnerabilidad de la sociedad moderna como el resultado inevitable del proceso de modernización en sí mismo. El resultado de este proceso es que la vieja sociedad industrial está siendo reemplazada por una nueva sociedad del riesgo en la que, según plantea Beck, los conflictos sociales son menos sobre la distribución de la riqueza y que sobre de la distribución de los riesgos.

La vulnerabilidad de la cultura tecnológica

En los apartados precedentes he revisado varias concepciones de la vulnerabilidad, cuando es aplicada a los sistemas técnicos y a las sociedades, y lo he realizado desde una perspectiva cultural. Revisaré ahora qué nos ha dado este análisis, focalizándome en la cultura tecnológica en sí misma. Tal como se mencionó previamente mi concepción de la cultura tecnológica aspira a subrayar: a) que rasgos característicos de nuestra cultura son penetrante e irrevocablemente tecnológicos; b) que nuestras tecnologías son completamente culturales; c) que solo podemos comprender nuestra sociedad moderna, altamente tecnológica, reconociendo el modo en que sus valores culturales dominantes y su tecnología se forman entre sí. Un estudio de la cultura tecnológica complementa un análisis de la sociedad tecnológica porque un estudio de tal tipo se focaliza en los valores culturales, las identidades y las prácticas que apuntalan las instituciones en estas sociedades.

La vulnerabilidad depende, en última instancia, de los valores. El ejemplo más crudo es una cultura que no valora las vidas humanas –una cultura de este tipo sería mucho menos vulnerable a los riesgos que pueden producir bajas, o a ataques terroristas que apuntan a matar personas. Los valores culturales varían ampliamente a lo largo del tiempo histórico y el espacio geográfico. La experiencia y el concepto de vulnerabilidad varían de acuerdo a ellos. Es trivial notar que a lo largo del siglo pasado un incremento en las condiciones de higiene en el mundo de los países ricos ha disminuido la vulnerabilidad humana a las enfermedades; es igualmente trivial observar que la vulnerabilidad de los individuos es muy diferente dependiendo de dónde viven. Las condiciones sociales, económicas y de salud son tan distintas en África, comparadas con las partes más ricas del mundo, que la vulnerabilidad debe tener allí un significado completamente diferente. Como plantea la filósofa del derecho Judith Shklar:

> […] lo que es visto como controlable y social es muchas veces un asunto de tecnología y de ideología o interpretación. La percepción de las víctimas y la de aquellos que, aún remotamente, pueden ser victimarios, tienden a ser bastante diferentes (Shklar, 1990:1).

Shklar construye su análisis acerca de la vulnerabilidad y la condición de víctima, acerca de la desgracia y la injusticia, sobre la observación de que: "la diferencia entre la desgracia y la injusticia frecuentemente involucra nuestra buena voluntad y nuestra capacidad para actuar o no actuar de parte de las víctimas, culpar o absolver, ayudar, mitigar, y compensar, o solo apartarse" (Shklar, 1990: 2).

Las diferencias en lo que hace a la vulnerabilidad entre diferentes regiones geográficas también pueden ser causadas por circunstancias políticas y relaciones de poder. Por ejemplo, tanto los palestinos como los israelíes se sienten vulnerables, pero el carácter de sus experiencias de vulnerabilidad parece ser bastante diferente. En un artículo para la cumbre de los Jefes de Estado de África, el Caribe y el Pacífico (ACP),[9] Fei Tevi amplía la vulnerabilidad a lo económico y lo social, y quiere "definir vulnerabilidad en relación al ambiente, la economía y la sociedad de la región del Pacífico" (Tevi, 1997: 1). La base para esta ampliación fue sentada en la Conferencia de las Naciones Unidas sobre Ambiente y Desarrollo (UNCED) de 1992 en Río de Janeiro, cuando "las naciones en desarrollo de las pequeñas islas fueron reconocidas como un caso especial para el ambiente y el desarrollo bajo la Agenda 21 debido a su vulnerabilidad, fragilidad, pequeño tamaño, dispersión geográfica y aislamiento" (Tevi, 1997: 14).

Tevi argumenta que reconocer esta vulnerabilidad es simplemente un asunto de supervivencia. Utilizando los conceptos de Wackers y Kørte, ahora podemos especificar esta "supervivencia": apunta al mantenimiento de integridad funcional como una comunidad, como una economía y como un pueblo. La supervivencia y la vulnerabilidad se relacionan aquí a la sustentabilidad –sustentabilidad en términos de energía y de ciclos de materiales, y en términos de seguridad existencial.

La variabilidad histórica de la vulnerabilidad, así como el hecho de que la vulnerabilidad es un concepto con carga valorativa, está muy bien ilustrado por la discusión acerca de lo que debería catalogarse como patrimonio cultural protegido. Por ejemplo, el valor histórico de las fortificaciones que fueron construidas por el ejército de ocupación alemán en los Países Bajos durante la Segunda Guerra Mundial, y que fueron declaradas patrimonio cultural. Si bien las fortificaciones de hormigón armado no son consideradas normalmente como vulnerables, tal decisión preservó estos edificios declarándolos vulnerables y que ameritaban ser protegidos.

El riesgo de epidemias como la del síndrome respiratorio agudo severo (SARS, gripe aviar) puede explicarse en los términos de Perrow, pero el sentido de vulnerabilidad que creó en 2003 puede describirse solamente refiriéndose a una idea dominante de salud completa que existe en nuestra cultura tecnológica. Una epidemia de SARS ciertamente puede analizarse como un sistema complejo con elementos tales como la venta y la manipulación de ganado (pollos, civetas) para consumo en mercados concurridos; la matanza

[9] La política de desarrollo de la Unión Europea está particularmente orientada hacia estos países.

doméstica de animales –con la subsecuente exposición de los humanos a sangre y entrañas–; la creciente probabilidad de nuevos virus emergentes a partir de la recombinación de virus de pollo y virus de influenza humanos; y el incremento en la movilidad física de seres humanos a través de unos pocos aeropuertos centrales (Singapur, Hong Kong). El impacto público de la epidemia de SARS de 2003 –inclusive en países del mundo occidental donde se produjeron pocas muertes– no fue resultado sin embargo de ciudadanos que hacían dicho análisis de riesgo. La epidemia tuvo tal impacto y creó tal agudo sentido de vulnerabilidad porque muchas personas en las partes más ricas del planeta pensaron que las enfermedades infecciosas estaban excluidas o confinadas a grupos específicos de personas y de tipos de comportamiento (como en el caso del VIH).

Si la vulnerabilidad es una característica inevitable de la cultura tecnológica, tal como yo pienso, entonces: ¿cómo manejan las culturas tecnológicas esta vulnerabilidad?

Con seguridad todas las rutinas de los ingenieros, los métodos científicos y las estrategias directivas juegan un papel, el cual hemos revisado en el contexto de los sistemas tecnológicos y las sociedades. Pero, ¿qué puede identificarse en el nivel de la cultura tecnológica? Pienso que la aproximación preventiva es al menos una respuesta parcial a este problema. Con un enfoque precautorio, las culturas tecnológicas pueden encontrar vías para vivir con su vulnerabilidad sin traicionar necesariamente sus valores fundamentales.

Probablemente, la versión del principio precautorio que ha sido más citada es la de la declaración de Río: "Allí donde hay amenazas de daños serios o irreversibles, no debería usarse la falta de una certeza científica plena como razón para posponer medidas rentables para prevenir la degradación ambiental" (Naciones Unidas, 1992). Esto implica un cambio, de la prevención de peligros claros y manifiestos a acciones preventivas para evitar riesgos hipotéticos: el principio permite interferir incluso cuando no es claro cuál es exactamente el riesgo. Desde entonces se ha desarrollado una abundante literatura que traduce este principio en varias aproximaciones preventivas (Gee y Jiménez Beltrán, 2001; Klinke y Renn, 2002). Lo que es importante para mis propósitos aquí es que en algunas versiones de un enfoque precautorio no solo se proponen formas de manejar los riesgos, sino que también se citan explícitamente los valores centrales de las culturas tecnológicas modernas. Por ejemplo Sue Mayer y Andy Stirling argumentan que su enfoque "reconoce la *complejidad* y la *variabilidad* del mundo real y encarna una cierta *humildad* en torno a los procedimientos y el conocimiento científicos" (Mayer y Stirling, 2002: 60, itálicas en el original).

Estos valores no necesariamente serán los mismos en todos los enfoques que se declaran precautorios, ni la implementación de valores específicos será incontrovertida y sin costos. Henk van den Belt y Bart Gremmen citan a Aaron Wildavski (1995), cuando advierten:

> […] contra la creencia ilusoria de que adhiriendo algo valioso al Principio Precautorio, la inteligencia humana o el bienestar medioambiental, puede obtenerse virtualmente a un costo absolutamente nulo, asumiendo con facilidad que las prohibiciones y regulaciones propuestas en sí mismas no tendrán efectos adversos para la salud (Van den Belt y Gremmen, 2002: 107).

La interpretación y la implementación del principio precautorio variarán inevitablemente, de acuerdo a las doctrinas legales y científicas, y a la apertura de la cultura política.

De tal modo la implementación particular del principio precautorio permite formar una cultura tecnológica de un modo específico. También nos conecta con mis señalamientos iniciales, en las cuales vinculé la vulnerabilidad con la innovación. La implementación del principio precautorio conforma un campo de batalla para el estímulo o la restricción de las innovaciones. Los críticos del principio precautorio temen que el mismo restrinja la innovación.

> La razón es que conduce a sus protagonistas a focalizarse principalmente en la posibilidad de que nuevas tecnologías puedan plantear –teóricamente– riesgos, previniéndose siempre contra los peores resultados posibles en los peores escenarios, ignorando al mismo tiempo los beneficios potenciales de tales tecnologías o los riesgos reales, ya existentes, que podrían ser reducidos o eliminados por ellas (Van den Belt y Gremmen, 2002: 106-107).

El informe de la Agencia Ambiental Europea, en el cual fueron revisados doce casos del uso del principio precautorio, también vincula la precaución al reconocimiento de que vivimos en un mundo cambiante al mismo tiempo que tenemos acerca de él un conocimiento limitado: "un elemento clave en un enfoque precautorio sobre la legislación involucra una mayor buena voluntad para admitir la posibilidad de lo imprevisto. Esto no significa recurrir a la oposición total a la innovación" (Gee y Jiménez Beltrán, 2001: 169).

Una última vía para rastrear el significado de la vulnerabilidad es preguntar cuál sería su opuesto. La oposición a la vulnerabilidad puede formularse como una pretensión de "resguardo" o "seguridad". Claramente la elección de las palabras, cuando se formula la meta de ofrecer una alternativa a la vulnerabilidad de la sociedad, no es inocente: sociedad sin peligro, sociedad segura, sociedad custodiada, o sociedad resiliente –estos términos admiten diferentes valo-

res y estrategias políticas. Las concepciones acerca de la vulnerabilidad caen en dos clases, dependiendo si el término opuesto tiene una connotación de *control* (tal como en seguridad) o *flexibilidad* (tal como en resiliencia).

Algunos ejemplos de reacciones hacia la vulnerabilidad que están orientados al control pueden ser las leyes sobre inmigración más estrictas y las tecnologías de administración y control que han sido recientemente instaladas en los Estados Unidos.[10] Tal como han argumentado diversas organizaciones, a la larga esto puede estorbar el desarrollo del conocimiento y la comprensión transcultural (*cross-cultural*) entre diferentes comunidades internacionales –y de tal modo incrementando posiblemente la vulnerabilidad de los Estados Unidos en el sentido de no ser capaz de reaccionar flexiblemente a las amenazas.[11]

Un ejemplo de defensa contra la vulnerabilidad orientada hacia la flexibilidad es mantener una variedad de cosechas y medios de vida, más que concentrarse en una actividad económica. Imaginemos una villa en el Lago Victoria en África, donde la ayuda al desarrollo ha mejorado las tecnologías pesqueras que ofrecen un mayor control a los pescadores porque, por ejemplo, son menos vulnerables a las malas condiciones del tiempo. Una consecuencia no intencional, entonces, puede ser que las actividades de labranza devengan relativamente menos beneficiosas, induciendo por lo tanto a la gente a abandonar la tradicional combinación de actividades económicas. Entonces esto hará que la villa sea menos flexible para reaccionar a cambios en los precios del mercado mundial de pescados y de granos –haciendo a la villa más vulnerable en este otro sentido.

La Agencia Ambiental Europea también vincula su discusión sobre el principio precautorio a la flexibilidad. Reconoce que nuestras culturas tecnológicas están en un estado de "ignorancia social" en muchas cosas importantes que se relacionan con los desarrollos tecnológicos y científicos. Esta ignorancia social es contrastada con la "ignorancia institucional" –en la que se refiere a una situación donde la información relevante para una decisión está disponible en la sociedad, pero no está disponible para los que toman las decisiones– lo que puede remediarse disponiendo una comunicación más efectiva y un aprendizaje social.

[10] Véase el informe del comité *ad-hoc* de la Society for Social Studies of Science (Downey *et al.*, 2003).

[11] Véase por ejemplo el texto de M. R. C. Greenwood, rector de la University of California (Greenwood, 2002) y la declaración de Bruce Alberts, presidente de la National Academy of Sciences de los Estados Unidos, Wm. A. Wulf, presidente de la National Academy of Engineering de los Estados Unidos, y Harvey Fineberg, presidente del Institute of Medicine de los Estados Unidos (Alberts *et al.*, 2002).

> [La] condición de ignorancia social es más difícil de manejar. Este problema [...] requiere remedios bastante diferentes, involucrando la investigación científica y el fomento de una mayor diversidad, adaptabilidad y flexibilidad en las tomas de decisión y en las elecciones tecnológicas (Gee y Jiménez Beltrán, 2001: 171).

Las realizaciones de nuestra cultura tecnológica están inextricablemente vinculadas no solo a la vulnerabilidad, bajo la forma de la ocurrencia de accidentes tecnológicos y de desastres naturales, sino también a las experiencias asociadas de la desgracia o la injusticia:

> Nuestras expectativas tecnológicas son habitualmente muy altas, pero dado lo que han realizado las últimas dos generaciones, sospechamos indiferencia injustificada o falta de justicia cuando no hay nadie para protegernos contra las aún indómitas fuerzas de la naturaleza. De hecho no es culpa de los científicos o de los funcionarios públicos que ahora pueda hacerse poco, ni son culpablemente indiferentes a la epidemia en curso. Las víctimas, sin embargo, parece que encuentran más fácil soportar su desgracia si perciben tanto injusticia como mala suerte (Shklar, 1990: 65).

Poniendo el foco en la vulnerabilidad de la cultura tecnológica no solo estudiamos la frágil constitución de las sociedades modernas sino que también podemos capturar la fragilidad que es constitutiva de nuestra cultura tecnológica y, por lo tanto, de sus estructuras y valores centrales.

Más que tratar la vulnerabilidad como algo que debe ser evitarse, repararse y combatirse –como algo que es un punto de partida implícito y no cuestionado para la acción, como en el caso de las políticas actuales de los Estados Unidos que mencioné previamente– propongo tratar la vulnerabilidad con el respeto intelectual que merece.[12] Cualquiera pueda ser la obsesión actual con la protección y la seguridad, nunca nos encontraremos en un estado de completa invulnerabilidad. En verdad yo no quisiera vivir en una sociedad de este tipo. Estudiar la vulnerabilidad de la cultura tecnológica puede ayudarnos a comprender nuestras sociedades actuales y altamente desarrolladas.

BIBLIOGRAFÍA

Alberts, B., W. A. Wulf y H. Fineberg (2002), "Current Visa Restrictions Interfere with U.S. Science and Engineering Contributions to Important National Needs", Office of News and Public Information-The National Academies, Washington.

[12] Me he inspirado aquí en el pedido de Shklar para "tratar la injusticia con el respeto intelectual que merece" (Shklar, 1990: 17).

Disponible en: <http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=s12132002>, 13/06/2003.

Arquilla, J., D. F. Ronfeldt y U. S. Department of Defense (2001), *Networks and netwars: the future of terror, crime, and militancy*, Santa Monica, RAND Corporation.

Bal, R., W. E. Bijker y R. Hendriks (2002), *Paradox van wetenschappelijk gezag. Over de maatschappelijke invloed van adviezen van de Gezondheidsraad, 1985-2001*, La Haya, Gezondheidsraad.

Beck, U. (1992), *Risk society: towards a new modernity*, Londres/Thousand Oaks/Nueva Delhi, Sage [existe edición en español, Beck, U. (1994), *La sociedad del riesgo. En camino hacia otra sociedad moderna*, Barcelona, Paidós].

Bijker, W. E. (1995a), "Democratisering van de Technologische Cultuur (Inaugurele Rede)", Maastricht.

—— (1995b), *Of Bicycles, Bakelites and Bulbs. Toward a Theory of Sociotechnical Change*, Cambridge, The MIT Press.

Blaikie, P. M., T. Cannon, I. Davis y B. Wisner (1994), *At risk. Natural hazards, people's vulnerability, and disasters*, Londres y Nueva York, Routledge.

Bowker, G. C. y S. L. Star (1999), *Sorting Things Out. Classification and its Consequences*, Cambridge, The MIT Press.

Branscomb, L. M. (2002), "The Changing Relationship between Science and Government Post-September 11", en Teich, A. H., S. D. Nelson y S. J. Lita (eds.), *Science and Technology in a Vulnerable World* (Supplement to AAAS Science and Technology Policy Yearbook 2003), Washington, American Association for the Advance of Science, pp. 21-32.

Callon, M., P. Lascoumes y Y. Barthe (2001), *Agir dans un monde incertain. Essai sur la démocratie technique*, París, Le Seuil.

Castells, M. (1997), *The power of identity*, Malden, Blackwell [existe edición en español: Castells, M. (1997), *El poder de la identidad*, Madrid, Alianza].

—— (2000a) [1996], *The rise of the network society*, Malden, Blackwell [existe edición en español: Castells, M. (1998), *La sociedad red*, Madrid, Alianza].

—— (2000b) [1998], *End of millennium*, Malden, Blackwell [existe edición en español: Castells, M. (1998), *Fin de milenio*, Madrid, Alianza].

De Wilde, R., N. Vermeulen y M. Reithler (2002), *Bezeten van genen. Een essay over de innovatieoorlog rondom genetisch gemodificeerd voedsel*, La Haya, Wetenschappelijke Raad voor het Regeringsbeleid.

Downey, G., H. Gusterson y J. Summerton (2003), "U.S. Visa Policies and Scholarly Work", Committee on Immigration Policy and Scholarly Work, Society for Social Studies of Science, Baton Rouge, Society for Social Studies of Science. Disponible en: <http://www.4sonline.org/4S%20Immigration%20Policy%20and%20Scholarly%20Work.pdf>.

Edwards, P. N. (1996), *The Closed World. Computers and the politics of discourse in cold war America*, Cambridge, The MIT Press.

Epstein, S. (1996), *Impure Science. Aids, Activism, and the Politics of Knowledge*, Berkeley, University of California Press.

Fortun, K. (2001), *Advocacy after Bhopal: environmentalism, disaster, new global orders*, Chicago, University of Chicago Press.

Gee, D. y D. Jiménez Beltrán (eds.) (2001), *Late Lessons from Early Warnings: The Precautionary Principle 1896-2000*, Copenhague, European Environment Agency.

Gezondheidsraad (1995), *Niet alle risico's zijn gelijk*, La Haya, Gezondheidsraad.

—— (1996), *Risico, meer dan een getal: Handreiking voor een verdere ontwikkeling van de risicobenadering in het milieubeleid*, La Haya, Gezondheidsraad.

Godin, B. e Y. Gingras (2000), "What is scientific and technological culture and how is it measured? A multidimensional model", *Public Understanding of Science*, 9, (1), pp. 43-58.

Gottweis, H. (1998), *Governing Molecules. The Discursive Politics of Genetic Engineering in Europe and the United Status*, Cambridge, The MIT Press.

Greenwood, M. R. C. (2002), "Risky Business: Research Universities in the Post-September 11 Era", en Teich, A. H., S. D. Nelson y S. J. Lita (eds.), *Science and Technology in a Vulnerable World* (Supplement to AAAS Science and Technology Policy Yearbook 2003), Washington, American Association for the Advance of Science, pp. 1-20.

Guggenheim, M. y H. Nowotny, (2003), "Joy in Repetition Makes the Future Disappear. A Critical Assessment of the Present State of STS", en Joerges, B. y H. Nowotny (eds.), *Social Studies of Science and Technology. Looking Back, Ahead*, Dordrecht, Kluwer Academic Publisher, pp. 229-258.

Hecht, G. (1998), *The Radiance of France. Nuclear Power and National Identity after World War II*, Cambridge, The MIT Press.

Hickman, L. (2001), *Philosophical tools for technological culture: putting pragmatism to work,* Bloomington, Indiana University Press.

Keulartz, J., M. Korthals, M. Schermer y T. Swierstra (eds.) (2002), *Pragmatist Ethics for a Technological Culture*, Dordrecht, Springer.

—— (2004), "Ethics in Technological Culture: A Programmatic Proposal for a Pragmatist Approach," *Science, Technology and Human Values*, 29, (1), pp. 3-29.

Klinke, A. y O. Renn (2002), "A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies", *Risk Análisis*, 22 (6), pp. 1071-1094.

La Porte, T. (1998), "The United States air traffic system: Increasing reliability in the midst of rapid growth", en Mayntz, R. y T. P. Hughes (eds.), *The Development of Large Technical Systems*, Frankfurt, Campus Verlag, pp. 215-244.

Law, J. (2003), "Ladbroke Grove: Or How to Think about Failing Systems", mimeo.

—— y W. E. Bijker (1992), "Postscript: Technology, Stability, and Social Theory," en Bijker W. E. y J. Law (eds.), *Shaping Technology - Building Society. Studies in Sociotechnical Change*, Cambridge, The MIT Press, pp. 290-308.

Levin, M. y R. Williams (2003), "Forum on Rethinking Technology in the Aftermath of September 11", *History and Technology*, 19, (1), pp. 29-83.

Mayer, S. y A. Stirling (2002), "Finding a Precautionary Approach to Technological Developments - Lessons for the Evaluation of GM Crops", *Journal of Agricultural and Environmental Ethics*, 15, (1), pp. 57-71.

Mokyr, J. (2002), *The gifts of Athena: historical origins of the knowledge economy*, Princeton, Princeton University Press.

Naciones Unidas (1992), *Rio Declaration on Environment and Development*, Nueva York, Centro de Documentación de las Naciones Unidas.

Nowotny, H. (2003), "Introduction", folleto para la conferencia "Cultures of Technology and the Quest for Innovation", Essen.

Oudshoorn, N. y T. J. Pinch (eds.) (2003), *How users matter: the co-construction of users and Technologies*, Cambridge, The MIT Press.

Perrow, C. (1999) [1984], *Normal Accidents: Living with High-Risk Technologies*, Princeton, Princeton University Press.

Pinch, T. y W. Bijker (1984), "The Social Construction of Facts and Artefacts: or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other", *Social Studies of Science*, 14, (3), pp. 399-441.

Rochlin, G. I. (1991), "Iran Air Flight 655 and the USS Vincennes: Complex, Large-scale Military Systems and the Failure of Control", en La Porte, T. R. (ed.), *Social Responses to Large Technical Systems*, Dordrecht, Springer, pp. 99-125.

—— (1994), "Broken Plowshare: System Failure and the Nuclear Power Industry", en Summerton, J. (ed.), *Changing Large Technical Systems*, Boulder, Westview Press, pp. 231-261.

Schlager, N. (1994), *When technology fails: significant technological disasters, accidents, and failures of the twentieth century*, Detroit, Thomson Gale.

Schumpeter, J. A. (1939), *Business cycles; a theoretical, historical, and statistical analysis of the capitalist process*, Nueva York/Londres, McGraw Hill [existe edición en español: Schumpeter, J. A. (2002), *Ciclos económicos. Análisis teórico, histórico y estadístico del proceso capitalista*, Zaragoza, Prensas Universitarias de Zaragoza].

Shklar, J. N. (1990), *The faces of injustice*, New Haven, Yale University Press.

Shrader-Frechette, K. S. (1991), *Risk and rationality: philosophical foundations for populist reforms*, Berkeley, University of California Press.

Sloan, S. (1995), "Terrorism: How Vulnerable is the United States?", en Pelletiere, S. (ed.), *Terrorism: National Security Policy and the Home Front*, Carlisle, The Strategic Studies Institute del U.S. Army War College, pp. 51-62. Disponible en <http://nsi.org/Library/Terrorism/usterror.htm>.

Snook, S. A. (2000), *Friendly fire: the accidental shootdown of U.S. Black Hawks over Northern Iraq*, Princeton, Princeton University Press.

Tevi, F. (1997), "Vulnerabilidad: una realidad del Pacífico", Cumbre de los Jefes de Estado y Gobierno de África, Caribe y Pacífico, Libreville.

Van Asselt, M. B. A. (2000), *Perspectives on Uncertainty and Risk. The PRIMA Approach to Decision Support*, Dordrecht, Springer.

Van den Belt, H. y B. Gremmen (2002), "Between Precautionary Principle and 'Sound Science': Distributing The Burdens of Proof", *Journal of Agricultural and Environmental Ethics*, 15, (1), pp. 103-122.

Vaughan, D. (1996), *The Challenger Launch Decision. Risky Technology, Culture, and Deviance at NASA*, Chicago, University of Chicago Press.

Verran, H. (2001), *Science and an African logic*, Chicago, University of Chicago Press.

Wackers G. L. y J. Kørte (2003), "Drift and Vulnerability in a Complex Technical System: Reliability of Condition Monitoring Systems in North Sea Offshore Helicopter Transport", *International Journal of Engineering Education*, 19, (1), pp. 192-205.

Watson-Verran, H. y D. Turnbull (1995), "Science and Other Indigenous Knowledge Systems", en Jasanoff, S., G. E. Markle, J. C. Petersen y T. Pinch (eds.), *Handbook of Science and Technology Studies*, Thousand Oaks, Sage, pp. 115-139.

Wildavski, A. (1995), *But Is It True? A Citizen's Guide to Environmental Health and Safety Issues*, Cambridge, Harvard University Press.

Artículo recibido el 30 de abril de 2007.
Aceptado para su publicación el 30 de enero de 2008.

Wiebe Bijker es uno de los teóricos más significativos de la sociología de la tecnología constructivista. Junto con Trevor Pinch organizaron el seminario de Twente que culminó con la edición de *The Social Construction of Technological Systems* (coeditado con T. Pinch y T. Hughes). En 1995 publicó *Of Bycicles, Bakelites and Bulbs,* una aproximación a la construcción de una teoría de la innovación tecnológica. En la actualidad dirige el Departamento de Ciencias Sociales y Tecnología, en la Facultad de Artes y Cultura de la Universidad de Maastricht, Holanda.