When vulnerability becomes an asset: revisiting Beck's risk society in the cyber age

Jong, Wouter

AI & SOCIETY
https://doi.org/10.1007/s00146-026-03256-7

CURMUDGEON CORNER

When vulnerability becomes an asset: revisiting Beck's risk society in the cyber age

Wouter Jong[1]

Received: 20 June 2026 / Accepted: 10 July 2026

Dear Editor,

I grew up academically with Ulrich Beck's idea of the *Risk Society*. His central insight was that modern societies create the very risks they later have to manage. Nuclear energy creates prosperity, but also the possibility of nuclear accidents. Industrialization creates wealth, but also pollution and environmental degradation (Beck 1992).

Beck also observed that many modern risks become increasingly detached from the places in which they originate. Radioactive fallout does not stop at national borders. Environmental pollution does not remain confined to the factory that produced it. The risks of modernity become disembedded from their original context and spread through increasingly interconnected societies.

Our response to these risks was remarkably consistent. We sought to identify the vulnerabilities that generated them and intervene at their source. The logic was simple: reduce the vulnerability and reduce the risk.

For decades, risk and crisis management have been built around that logic. Commercial aircraft are designed with multiple redundant systems so that a single failure does not bring down the plane. Chemical plants are engineered to prevent dangerous substances from mixing. A truck carrying hydrochloric acid could only connect to the correct storage tank. If the driver attempted to unload the cargo into another tank, the hose simply would not fit. Simple. Effective. Usually enough to prevent an unwanted explosion.

Underlying all these efforts is a simple assumption: risks may originate outside the system, but vulnerabilities reside within it. Floods threaten dikes, human error threatens railway systems, and accidents threaten chemical plants. The source of the threat may be external, but the vulnerability remains embedded in the system itself.

That assumption has made our societies significantly safer. And if we are not careful, we may approach artificial intelligence through exactly the same lens: a new technology, new risks, and therefore new safeguards designed to reduce vulnerabilities and contain risk.

I believe that is where we may be making a fundamental mistake. For generations, discovering vulnerabilities has been regarded as a way of reducing risk. In cyberspace, that assumption can no longer be taken for granted.

A dike can be vulnerable. Yet there is no global marketplace where weaknesses in flood defenses are bought and sold. There is no exchange where engineers bid on flaws in railway signaling systems. Nor is there a market where, for the right price, someone will tell you which bridge is most likely to collapse next year.

Cybersecurity is different. And artificial intelligence amplifies that difference. The difference is not simply that cyber vulnerabilities can be traded. It is that discovering vulnerabilities no longer automatically makes systems safer.

A software vulnerability can become detached from the system in which it was discovered. Once identified, knowledge about that vulnerability can be copied, stored, shared, sold, auctioned, and reused. A zero-day vulnerability may be worth thousands or even millions of dollars. Entire markets have emerged around the discovery, valuation, and exchange of vulnerabilities.

This is what makes cyber vulnerabilities fundamentally different from most vulnerabilities studied in risk and crisis management. They no longer remain tied to the infrastructure in which they originate. Once detached, they can circulate independently.

In that sense, Beck's idea of disembedded risk may need to be revisited. What we are witnessing today is not merely the globalization of risk. It is the emergence of disembedded vulnerabilities.

✉ Wouter Jong
w.jong@fgga.leidenuniv.nl

[1] Institute of Security and Global Affairs, Leiden University, The Hague, Netherlands

Published online: 24 July 2026

That may sound like a subtle distinction, but it changes the nature of risk itself.

In Beck's world, risks became detached from the places in which they originated. A nuclear accident in one country could affect populations far beyond its borders. Yet the vulnerabilities that generated those risks remained embedded in the systems themselves. The reactor was still located somewhere. The flaw remained attached to a physical object. For decades, identifying vulnerabilities was almost synonymous with reducing risk. If inspectors discovered a weakness in a bridge, a flaw in a railway signaling system, or a safety issue in a nuclear power plant, the solution was straightforward: fix the vulnerability and make the system safer.

As vulnerabilities become detached, organizations no longer have a monopoly on discovering vulnerabilities in their systems. Vulnerabilities may be identified by security researchers, competitors, criminals, or intelligence services operating far beyond the organization itself. Artificial intelligence accelerates this process.

The result is a paradox that Beck could hardly have anticipated, because cybersecurity introduces a different dynamic where vulnerability itself becomes a source of vulnerability.

Traditionally, discovering vulnerabilities was a risk-reducing activity. In cyberspace, vulnerability discovery reduces risk for defenders, but increases opportunities for attackers. Perhaps the defining feature of the cyber risk society is therefore not simply that it produces new risks. Perhaps it is that the very act of discovering vulnerabilities, long regarded as a cornerstone of safety and risk reduction, has itself become a source of risk.

If that is the case, risk scholars may need to rethink one of their most fundamental assumptions. Vulnerabilities are no longer merely properties of systems. Increasingly, they are objects that circulate independently of those systems.

For decades, risk management focused on vulnerable systems. The cyber age may require us to focus on vulnerability discovery and the markets, networks, and actors through which vulnerabilities circulate.

Author contributions Single author; WJ all.

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no competing interests.

Curmudgeon Corner Curmudgeon Corner is a short opinionated column on trends in technology, arts, science and society, commenting on issues of concern to the research community and wider society. Whilst the drive for super-human intelligence promotes potential benefits to wider society, it also raises deep concerns of existential risk, thereby highlighting the need for an ongoing conversation between technology and society. At the core of Curmudgeon concern is the question: What is it to be human in the age of the AI machine? -Editor.

Reference

Beck U (1992) Risk society: towards a new modernity. Sage, London and New York