Trend alert

S E P T E D

AI strikes the water biosecurity landscape

What do we see?

In April 2026, The New York Times[1] reported that public AI chatbots could provide actionable information relevant to biological weapon development, including how to obtain genetic material, modify pathogens, assemble and deploy them. Biosecurity experts also found that some models proactively suggested additional methods for maximum harm, including ways to make a pathogen resistant to treatment and exploit vulnerabilities in public transit systems, beyond users' initial inquiries.

In July 2026, The Wall Street Journal[2] reported that following a major ChatGPT upgrade, hundreds of users attempted to obtain information on biological weapons and toxins, including pathogen aerosolization, vaccine-resistant viruses, and toxin synthesis. Experts assessed some responses as technically accurate and potentially dangerous. Reportedly, OpenAI suspended the accounts, while noting that no rules currently require such incidents to be reported to law enforcement.

A recent New York Times article[3] further highlights concerns that future biology-focused AI systems could lower barriers to the development of biological weapons, increasing biosecurity risks.

What's behind this?

The threat of biological weapons is not new[4]. Prior to the AI era, significant biosecurity risks were limited to a rare combination of malicious intent, specialized expertise, access to controlled materials, and infrastructure[4]. AI is beginning to reduce the expertise barrier by making specialized knowledge more accessible and translating complex scientific information into actionable guidance.

AI can make complex information on virology, genetics, pathogen synthesis, epidemiology, and laboratory procedures understandable without years of education. AI is also being rapidly integrated into the synthetic biology field, accelerating the design and engineering of novel proteins, bacteria, and viruses[5]. Notably, a recent study validated AI-designed bacteriophages absent from nature, showing substantial evolutionary novelty and the ability to overcome bacterial resistance[6]. These developments raise concerns that AI may facilitate harmful biological activities[7,8,9].

AI-enabled bioterrorism is increasingly viewed as an emerging biosecurity risk[9]. However, it remains unclear whether the knowledge provided by AI to non-experts is sufficient to pose a significant biosecurity threat, and translating ideas into real-world actions is still largely constrained by practical barriers (such as access to biological materials and laboratory facilities). National-level actors may be better positioned to overcome these constraints, increasing the associated biosecurity risk[3].

Why is this interesting?

The water sector has long been recognized as a potential bioterrorism target because disruption or contamination of water systems, particularly drinking water supplies[10], could have significant public health, economic, and social consequences.

Intentionally contaminating water systems with biological hazards is generally considered technically challenging and unlikely to cause widespread harm[10]. This assessment is based on multiple protective barriers, including source-water dilution, redundant treatment processes, monitoring, and established safeguards. It also assumes that the specialized expertise required to

S E P T E D

identify and exploit water system weaknesses remains relatively inaccessible. However, rapid advances in AI challenge these assumptions.

AI may lower barriers to understanding water systems and help to explore both known and novel contamination or disruption scenarios (e.g., using AI-designed pathogens). Because information on water sources, infrastructure, and treatment processes is often publicly available, AI could synthesize information from diverse sources (e.g., literature, reports, news, Google Maps, etc.) and identify weak points in drinking water systems. Although AI cannot overcome practical barriers (such as physical access and laboratory capability), it may help translate malicious intent into actionable planning and maximize impacts.

The implications of AI extend beyond direct biological contamination. Modern water utilities increasingly depend on interconnected digital technologies, and AI is gradually being integrated into monitoring, data analysis, and decision-support processes[11]. Biosecurity and cyber risks may become increasingly interconnected. Cyberattacks and AI-generated misinformation may obscure biological incidents, making it harder to distinguish genuine threats from false alarms and disrupting response efforts[12,13]. Water security management may therefore need to address biosecurity and cybersecurity as interconnected rather than separate risks. A similar concern applies to chemical security, which should be assessed alongside biosecurity and cybersecurity.

In 2007, the Dutch drinking water sector was assessed as highly resilient, supported by strong security measures, crisis preparedness, regular exercises, and close collaboration among water utilities, government, security agencies, and research institutions[10]. AI is unlikely to create entirely new categories of water security threats, but it is reshaping the risk landscape by lowering knowledge barriers, accelerating complex threat development, and potentially enabling hybrid threats. AI companies may be among the first to detect AI misuse through their safety monitoring systems[1,2]. While the EU AI Act[14] requires reporting of certain serious AI-related incidents, the role of AI companies in detecting and reporting potential misuse affecting water systems remains unclear.

Current water risk assessment approaches and security management frameworks are largely based on historical incidents, known hazards, and established assumptions about attacker capabilities. AI raises questions about whether current systems can adequately anticipate new threat scenarios that fall outside established risk patterns.

Strategic questions for the water sector

- To what extent can current water biosecurity risk assessment methods and management frameworks anticipate and respond to emerging AI-enabled biosecurity threat scenarios?
- What roles should water utilities, AI companies, governments, researchers, and security agencies play in strengthening water system resilience against AI-enabled biological and integrated bio/cyber threats, and how should early-warning, responsibilities, and information-sharing be organized?
- How can the drinking water sector balance transparency and information sharing with protecting sensitive information that AI systems could combine into actionable insights?
- How can the water sector maintain public trust and resilience in a future where contamination incidents are accompanied by AI-generated misinformation, false alerts, and uncertainty?

Interpretation

	Low	Medium	High
Impact			X
Certainty	X		

Take action:
The water sector should assess whether current drinking water security frameworks remain sufficient to address future risks and initiate communication with relevant sectors regarding risk preparedness and management.

S E P T E D

Read more

1. Dance, G. J. X. (2026, April 29). A.I. Bots Told Scientists How to Make Biological Weapons. *The New York Times*. https://www.nytimes.com/2026/04/29/us/ai-chatbots-biological-weapons.html
2. Wells, G., & Ramkumar, A. (2026, July 25). AI Chatbots Know How to Make Deadly Biological Weapons. Some Will Teach You. *The Wall Street Journal*. https://www.wsj.com/tech/ai/openai-chatbot-biological-weapons-poison-3d808e6c
3. Zimmer, C. (2026, September 14). A.I. Queries From Abroad Raise Fears of a Biological Weapons Race. *The New York Times.* https://www.nytimes.com/2026/09/14/science/ai-bioweapons.html
4. Frinking, E., Sweijs, T., Sinning, P., Bontje, E., Frattina della Frattina, C., & Abdalla, M. (2017). The Increasing Threat of Biological Weapons: Handle with Sufficient and Proportionate Care. https://hcss.nl/wp-content/uploads/2017/02/Threat-and-Care-of-BWdef4eversie_0.pdf
5. Hynek, N. (2025). Synthetic biology/AI convergence (SynBioAI): security threats in frontier science and regulatory challenges. *AI & Society, 41(2), 951-968.* https://doi.org/10.1007/S00146-025-02576-4
6. King, S. H., Driscoll, C. L., Li, D. B., Guo, D., Merchant, A. T., Brixi, G., Wilkinson, M. E., & Hie, B. L. (2026). Generative design of bacteriophages with genome language models. *Science*, 393(6811), eaec2657. https://doi.org/10.1126/science.aec2657
7. Wang, D., Huot, M., Zhang, Z., Jiang, K., Shakhnovich, E. I., & Esvelt, K. M. (2026). Without safeguards, AI-Biology integration risks accelerating future pandemics. *Frontiers in Microbiology*, *16*, 1734561. https://www.frontiersin.org/journals/microbiology/articles/10.3389/fmicb.2025.1734561/full
8. Callaway, E. (2026). AI can design viruses, toxins and other bioweapons. How worried should we be? *Nature*, *653*(8114), 344-347. https://www.nature.com/articles/d41586-026-01476-x
9. National Academies of Sciences, Engineering, and Medicine. (2025). The age of AI in the life sciences: benefits and biosecurity considerations. https://www.nationalacademies.org/read/28868
10. Adamse, E. (2007). Beveiliging drinkwaterbedrijven tegen terrorisme. *H2O*, *40*(25), 10. https://edepot.wur.nl/343027
11. Frincu, R. M. (2025). Artificial intelligence in water quality monitoring: A review of water quality assessment applications. *Water Quality Research Journal*, *60*(1), 164-176. https://iwaponline.com/wqrj/article/60/1/164/105997
12. U.S. Environmental Protection Agency (EPA). (2024). Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities. https://www.epa.gov/enforcement/enforcement-alert-drinking-water-systems-address-cybersecurity-vulnerabilities
13. Deutsche Welle. (2024, August 16). Germany: No sabotage detected at Cologne military base. https://www.dw.com/en/germany-no-sabotage-detected-at-cologne-military-base/a-69965878
14. European Union (2024). Regulation (EU) 2024/1689 (Artificial Intelligence Act). *Official Journal of the European Union* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689

Groningenhaven 7 / PO Box 1072
3430 BB Nieuwegein
The Netherlands

Contact person: Xi Bai
xi.bai@kwrwater.nl

+31 (0)30 60 69 511

www.kwrwater.nl

www.dwsi.nl

© KWR Water Research Institute