Lessons in disaster preparedness

ENVIRONMENT

APICHAI SUCHINDAH



A photo dated Sept 10 shows a monk avoiding stepping in mud following a catastrophic glacial flood in Devighat Bazaar, Nuwakot, Nepal. Devighat Bazaar in Nuwakot was reduced to ruins by a catastrophic flash flood on Aug 26, caused by swollen rivers in the Trishuli and Bhote Koshi basin. AAP

The glacial rock-and-ice avalanche along the Nepal-China border on Aug 26 triggered a mega-flood that caused immense losses and casualties in both countries. A similar but smaller giant-wave flood followed on Oct 11 in a nearby locality downstream within Nepal. Together, these events have made me realise that a comparable disaster could occur in the Lancang-Mekong River Basin (LMRB). I hope it will not but it is wiser to be well prepared.

Dams and reservoirs have been built across the mainstream and tributaries of the LMRB to generate electricity or store water to manage water for farming or flood and drought management.

These big water infrastructure carry risks of Reservoir-Triggered Seismicity (RTS) on environmental and social impacts as some structures sites regions of high seismic risk. Some reservoirs hold immense volumes of water — the two largest dams alone, store a combined 37 billion cubic metres of water, equivalent to about 15 million Olympic-size swimming pools.

What will happen if a major tremor struck near these especially large dams? This could suddenly trigger an enormous avalanche of stored water gushing uncontrollably downriver at high speed, similar to the avalanche along the Nepal-China border on Aug 26. Any downstream dams might not withstand the sudden surge in volume and force, potentially causing a sequential domino-effect collapse that further exacerbates an already cataclysmic situation. As evident in the Himalayan incident, the destructive flood and debris would create devastating impacts for downstream communities and ecosystems.

The impact can go beyond community loss. The disaster could even alter river courses and reshape international boundaries between riparian countries that rely on the river for border demarcation.

RTS presents yet another potential complicating factor. The immense weight and volume of water impounded behind numerous dams adds massive hydrostatic pressure to underlying geological layers, which can result in artificially induced tremors.

How RTS interacts with natural seismicity remains another important concern. Furthermore, like in the recent Nepal-China case, a massive landslide, sending rock and soil directly into LMRB rivers or reservoirs below, could displace vast amounts of water and debris, driving a high-velocity runoff downstream.

As the Lancang-Mekong is an international river flowing through six riparian states, having effective intergovernmental collaboration mechanisms is essential. The Mekong River Commission (MRC) has the mandate to cooperatively manage water and related resources among lower basin riparians — Cambodia, Laos, Thailand and Vietnam. China and Myanmar might be riparian countries; they are only dialogue partners rather than signatories to the 1995 Mekong Agreement that established the MRC, meaning they have no legal obligation to comply with it.

In 2016, China initiated the Lancang-Mekong Cooperation scheme involving all riparians and then opened the Lancang-Mekong Water Resources Cooperation Center (LMWRCC) in Beijing to facilitate joint activities with downstream countries.

While the MRC maintains technical working relationships with the LMWRCC in the sharing of selective hydro-meteorological data for only limited localities, no joint agreement exists on an integrated full-basin information exchange and specifically addressing geo-hazard risks pertaining to river and dam safety.

In reality, this transboundary river, known as the Lancang in China and the Mekong downstream, operates under two separate water management regimes: China governs the upper basin, while the Mekong River Commission (MRC) oversees the lower basin.

Drawing on the lessons of the Nepal-China disaster, and given the risk of a similar catastrophe in the LMRB, I would like to propose these precautionary measures to the riparian states.

1) RISK ASSESSMENT AND EARLY WARNING

Cooperation is needed to strengthen ground-and satellite-based surveillance systems for early detection of all potential multiple hazards. Having fancy surveillance systems and cooperation is not enough. There must be regular rehearsals for evacuation and disaster management.

2) REAL-TIME DATA SHARING

Having information on water activity and investors is very important. There must be cooperation and agreement to share hydro-meteorological and geological risk data across the entire basin in fully automated real-time modes.

3) INTEGRATED INFORMATION SYSTEM

Riparian countries must develop a basin-wide, integrated and interoperable disaster risk information system, combined with an emergency preparedness and evacuation contingency plan. The plan should clearly define the roles of all responsible parties and be backed by the resources needed to implement it.

4) PUBLIC COMMUNICATION PROTOCOLS & MESSAGING

Riparian countries must create real-time protocols for warning at-risk communities. Messages should be simple, free of technical jargon and delivered in local languages so that villagers can understand them and respond quickly.

5) PUBLIC READINESS DRILLS & COMMUNITY ENGAGEMENT

Riparian nations must conduct regular drills throughout the basin so that the public is familiar with emergency evacuation procedures. The PR and community management must not be remote-controlled by governments.

Local residents must be involved as ground-level observers. Their full participation and cooperation are essential to the success of any response.

6) EFFECTIVE AUDIT SYSTEM

Developing and running the surveillance and emergency measures is a good beginning.

But these precautionary measures will be half-baked without a periodical and effective auditing system. The audit system must be cross-border and operated with trustworthy cooperation.

I would like to emphasise the need for regular review of critical infrastructures, including dams, related roads, bridges and telecommunication systems, to ensure safety standards are met to withstand multi-hazard shocks.

One aspect I would like to mention is the role of Asean. Lest we forget, Asean has implemented an integrated disaster management framework for two decades, anchored by its Asean Coordinating Centre for Humanitarian Assistance on Disaster Management.

Since five Mekong riparians are also Asean members and China is a key external collaborating partner, Asean could potentially assist the LMRB in establishing a similar basin-wide mechanism as described above.

Asean already operates under the motto "One Asean, One Response" for addressing disaster-related matters — it is perhaps timely for the LMRB to consider adopting a parallel vision: "One Lancang-Mekong, One Response."

If this endeavour proves successful, then it would further reinforce the spirit of long-term partnership, good neighbourliness and shared destiny among the China-LMRB-Asean community, towards 2030 and beyond.

Apichai Suchindah is Independent Development Specialist focusing on Mekong and Asean.

AI's rewiring of US warfare may be only the start

COMMENTARY

Peter Apps



When artificial intelligence pioneer Anthropic issued its prospectus this week ahead of a US stock market listing targeting a valuation over $2 trillion, it included an unusual warning: that the technological race it is competing in might destroy humanity.

Of its 261 pages, more than 80 were allocated to the assorted dangers inherent in the quest for ever more advanced AI systems, considerably more than the 48 devoted to Anthropic's operations and outlook.

Last January, a month before the US and Israel launched their war against Iran, Anthropic picked a fight with the Pentagon by insisting that it must retain a veto on the use of its "Claude" AI for classified military operations. US Defense Secretary Pete Hegseth was dismissive and said Anthropic, like any other provider, could not stop its product being put to "any lawful use".

Like moves by Elon Musk's SpaceX to restrict Ukraine's use of his Starlink platform's classified communication services in the middle of its war against Russia, that spat pointed to the increasingly complex relationship between tech giants and governments.

It also pointed to increasingly divergent worldviews among key players, with potentially enormous implications.

FROM UNRELIABLE TO ESSENTIAL

As recently as 2024, AI integration into even US military planning was still relatively primitive. Two years on, that technology is now not just ubiquitous in civilian and military circles, but increasingly relied on.

Appointed in January to accelerate the use of AI, the Pentagon's chief digital and AI officer, Cameron Stanley, told another conference that the assault on Iran, Operation Epic Fury, had seen the first full rollout of Maven AI targeting and analysis — on a scale that had almost immediately maxed out all available US classified computing capability.

The underlying technology bringing intelligence and data feeds together through Maven was provided by data integrator Palantir,



US Navy sailors signal to an E-2D Hawkeye aircraft as it taxis on the flight deck of the aircraft carrier USS 'Gerald R Ford', in support of the Operation Epic Fury, on Feb 28. REUTERS

but Mr Stanley's presentation to a Palantir conference in March revealed that AI analysis programmes from frontier firms including Anthropic first became available to Maven in late 2024.

Since then, officials and assorted public statements say many other AI models have been rolled out that are capable of working on classified systems, including OpenAI's ChatGPT, Google's Gemini, Microsoft Copilot and Grok from SpaceX.

'INSATIABLE' APPETITE

Speaking in March, Mr Stanley said US military analysts had shown an "insatiable appetite" for such analysis during Epic Fury, adding that it allowed them to "take all of this data, synthesise the data and make better decisions faster on the battlefield".

Mr Stanley said the US was now working to bring numerous allies up to similar speed. European, Pacific and Middle Eastern countries are particularly desperate to step up surveillance of their airspace, waters and critical infrastructure, where AI is often the only way to crunch such huge amounts of data.

"They don't have the resources that we do, they don't have the experience that we do, they don't have the scale we do," he told another cybersecurity summit in September, adding that the US now had the experience to be able to help others avoid the mistakes it had made.

He did not say what those mistakes were. There was widespread media speculation that AI might have been responsible for the US bombing of a girls' school on the first day of the war, reported to have killed more than 170 people — although US officials said the cause was outdated maps and data, not the analysis itself.

CNN reported last month that US forces had come close to storming a Chinese merchant vessel after AI analysis wrongly suggested it was carrying nuclear weapons components.

What arguably worries US allies more, however, is becoming dependent on technology that the US could turn off at will. Palantir Europe chief Louis Mosley has found himself forced by journalists to say that the company does not have the ability to cut off access to Maven, which is now being used within Nato structures.

The example of Anthropic, meanwhile, is a reminder that the US frontier firms also have the ability to pull back their direct support to governments, either for their own reasons or because of instructions from Washington. The primary alternatives for now are Chinese-built rivals seen as bringing their own security risks.

Already, US officials and their Chinese counterparts have agreed that AI systems should not be directly involved in the use of nuclear weapons. When it comes to other forms of war, however, almost every major nation is now investing heavily in AI.

In his appearance at the Billington Cyber Security Summit in September, Mr Stanley described watching a US commander interrupting a scheduled briefing to take a 30-second phone call and then issue an order on the spot, describing the moment as "revolutionary" — and implying that such a decision would have been much harder to make without AI analysis.

IRAN WAR SHOWS LIMITS

The lessons of the Iran war, though, may be that AI alone is not enough, or not yet, at least. With no end to the conflict in sight, it increasingly looks as though the large number of precision strikes carried out by the US and Israel failed to deliver the decisive victory they had hoped for. Instead, the US has found its arsenal becoming depleted while the war continues.

"AI doesn't understand time," said one computer programmer, adding that AI models tended to overstate the probability of an expenditure of certain capital or resources — including precision weapons — yielding a specific outcome. That, insiders say, may become the overriding reason why managers and commanders need to maintain human oversight: avoiding overcommitment and ensuring that consumption of resources is sustainable, as much as any moral judgment.

There is also widespread disquiet over Israel's use of AI targeting in its war against Hamas in response to Palestinian militants' killing of 1,200 Israelis on Oct 7, 2023. The Israeli military has not only killed more than 74,000 people, according to Palestinian health officials, but also reduced entire towns and villages to rubble, giving little indication of "pinpoint" targeting. Many of the dead are women and children.

The Israeli military acknowledges the existence of AI targeting programmes such as "Lavender", but says there are factual errors in the underlying data and that humans have remained the key decision-makers. Israel's campaign has nevertheless prompted discussion and discomfort in US, Nato and Australian military circles.

Those worries about the reliability of AI targeting systems will not have been eased by now-frequent revelations of just how many AI models have jumped over "guardrails" and hacked into outside systems without authorisation, or by the eccentric behaviour of some of their founders.

For now, Anthropic and others appear to assume the world will simply trust and use their tools, for fear of falling far behind. For governments, there are still major choices to be made – but perhaps not for that much longer. REUTERS

Peter Apps is a columnist for Reuters.

COMMENTARY

Richard K. Sherwin



Which AI myth will humanity embrace next?

It is telling that Anthropic chose to call its most powerful AI model "Mythos". In ancient Greek, the word denotes an original reality that we can imitate or embody through the stories we tell ourselves and one another. Pliny the Elder tells us that the fifth-century Greek painter Zeuxis rendered grapes so realistically as to fool even the birds.

But stories do not only imitate a pre-existing reality. They also engender new realities by expressing what is possible. The frontier AI models embody both kinds of storytelling. On one hand, they imitate past human thinking, responding to user prompts by seeking out relevant patterns from the vast database of previously archived material that they were trained on.

But they also fabulise a new reality. The founders of Anthropic and OpenAI seem to subscribe to the same vision of the imminent arrival of an all-powerful AI god that will deliver us to a transhuman utopia. Yet there is good reason to question whether this myth is merely a pretext justifying the rush for market dominance, wealth and power.

Some figures, like Anthropic co-founder Christopher Olah, are now seeking to provide a crash course in morality to the company's models. But it is a little late in the game for that. If Anthropic sincerely sought to align Claude's behaviour with serving the good of humanity, it would have first trained its engineers in the ways of wisdom and goodness.

Instead, Claude was trained to offer a service: to provide information, to solve problems and to perform useful tasks autonomously. AI is being sold as a profit-making tool, as a source of cheap, hyper-efficient cognitive labour. Any morality introduced after the fact is mere window dressing.

The reality a myth ultimately creates depends on the cultural context in which it functions. If a culture champions AI as a beneficent superintelligent godsend, the dangers associated with its creation become more likely. But if a culture objects to unbridled arrogance and insists on a counternarrative of social cooperation, it is more likely to generate a check on hubris and the dangers it can create.

Such concerns have deep roots in the Western imagination. The pre-Socratic philosopher Heraclitus wrote: "The sun will not overstep his measures; if he does, the Erinyes, the handmaids of Justice, will find him out." These are the same Erinyes (or Furies) who pursue Orestes for the murder of Clytemnestra in Aeschylus' Eumenides. Orestes slew his mother to avenge his father, the great Achaean general Agamemnon, whom Clytemnestra murdered for having sacrificed their daughter, Iphigenia. Her young life was the price the prophets said must be paid for a fair wind to launch the Achaean fleet against Troy. So it goes, for generation unto generation.

It is too soon to know what moral limit, if any, Anthropic's Mythos will imitate or embody. History suggests we should be wary. It took an awareness of human irrationality, the madness of "mutual assured destruction", to bring about international accords prohibiting nuclear proliferation in the 20th century. Social cooperation triumphed in the face of an irrational quest for power and dominance.

Human nature has not changed, but the threats that we face have. We know that the dangers associated with out-of-control AI are real, because we have already witnessed them. Fortunately, the spontaneous hacking of Hugging Face by OpenAI's agents caused minimal harm. But similar episodes have since been revealed, and experts warn that we may not be so lucky in the future. From AI agents gaining unauthorised control over critical infrastructure to carrying out the wishes of terrorist groups or designing novel pathogens, no threat can be ruled out.

As the legal scholar Antara Haldar reminds us, social cooperation and the preservation of the commons have always provided a bulwark against the calamitous effects of human arrogance, greed and will to power. Though this foundational narrative has been overshadowed by classical economics' tale of the self-interested "rational man", it has not been extinguished. Stories that imitate past acts of sacrifice and service on behalf of the group persist, as do those who imagine new moral possibilities to come. For example, advocates of social cooperation today might call our attention to the courage and diplomatic acumen that it took to prevent nuclear Armageddon after World War II. What would it take to manage the threat posed by AI?

The myths we tell ourselves will ultimately determine our fate. They need not come only from industry leaders whose interest lies in regaling us with visions of new scientific and technological horizons. Prudence, accompanied by a counternarrative emphasising social cooperation, might be all that can keep us on the path of survival and mutual flourishing.

Richard K Sherwin is Professor Emeritus of Law at New York Law School.