# How do we navigate Asia-Pacific's climate-cyber polycrisis?

The effects of Typhoon Odette in Lapu-Lapu City, Cebu, Philippines, 2021
*Photo Credit: Unsplash/Carl Kho*

by Anne Cortez

26 February 2026

Communities globally are increasingly exposed to overlapping threats. Extreme weather, health emergencies and cyberattacks are occurring more frequently and simultaneously, often interacting in ways that amplify risks and strain response systems. Experts describe this as a polycrisis, where threats converge, creating a complex pressure point for governments, businesses and communities.

Today, a polycrisis is brewing at the intersection of climate change and cybersecurity. The latest Global Risks Report by the World Economic Forum ranks extreme weather and natural disasters among the top global threats, while risks linked to digital and artificial intelligence have climbed up the list. Over the next decade, these environmental and technological dangers are expected to dominate, underscoring how deeply intertwined they have become.

Asia and the Pacific is increasingly becoming a hotspot for these twin threats. The world's most disaster-prone region, it faced the highest number of disasters and deaths in 2023, with 66 million people affected and annual losses reaching an estimated US$780 billion. At the same time, the region has become the new ground zero for cybercrime, fuelled by rapid digital transformation during and after the pandemic. In 2024, it accounted for over one-third of all global cyber incidents, including roughly 135,000 ransomware attacks in Southeast Asia alone, costing the region an average of US$3.05 million per attack. The Philippines, Indonesia and Vietnam were among the most affected.

Asia's geographic exposure and rapid digital growth have turned its climate vulnerability into a growing cyber vulnerability, especially across critical infrastructure and information systems. As essential services including health, communications and energy depend on digital networks, climate-driven disruptions such as typhoons and floods can force systems into manual workarounds or less secure channels, creating openings for digital breaches at the worst possible moment. The 9.1 magnitude earthquake and tsunami in Japan in 2011 provided an early glimpse into the interconnected climate-cyber risks. In weeks following the

earthquake, cyber criminals exploited the chaos with phishing and malware schemes disguised as disaster relief efforts, stealing data and hindering recovery.

So far, cases in the region have largely involved natural hazards, but climate change is intensifying these events, increasing their frequency and severity and placing sustained stress on digital infrastructure, which in turn creates more openings for cyber attacks. Some researchers suggest that, contrary to prevailing beliefs, climate change is expected to increase the frequency and severity of earthquakes and volcanic eruptions in addition to other extreme weather events, and all of these events have been linked to spikes in cyber incidents.

Research shows that the likelihood of cyberattacks increases dramatically during natural disasters, as defensive systems and attention are compromised. In the United States, for instance, government agencies and researchers have warned the public of heightened digital threats including scams following hurricanes and wildfires, demonstrating how climate hazards can create openings for malicious actors. When these vulnerabilities are exploited, response and recovery efforts can be paralysed at the very moment they are most needed.

This convergence of vulnerabilities changes the nature of disaster risk. The UN Office for Disaster Risk Reduction now includes cyber threats in its hazard taxonomies because losses of connectivity and cyber incidents reshape exposure and coping capacity. Treating these threats separately leaves significant gaps in preparedness and response.

Across the Caribbean, interest in the climate-cyber convergence has grown, with governments and partners conducting assessments, dialogues and scenario planning to strengthen shared resilience and ensure that physical and digital systems can withstand compounded shocks. In Europe, researchers are drawing lessons from environmental law to inform and strengthen cybersecurity policies. Given these global developments, it is concerning that the recent COP30 focused heavily on how technology can support climate adaptation, yet paid less attention to how the same systems become vulnerable during climate-driven disruptions. Even more worrying is that Asia and the Pacific, despite being highly exposed to both disaster and cyber risk, has not yet shown the same level of integrated response or public alarm seen elsewhere.

The region has robust frameworks for disaster and climate resilience under the Sendai Framework for Disaster Risk Reduction, implemented through regional action plans, financing facility and cooperation programs. At the same time, ASEAN and its partners have cybersecurity policy guidelines that cover digital governance, data management and response to transboundary cyber threats. However, these

tracks largely operate in parallel, missing opportunities for integration. Reports highlight gaps in how climate and cyber risks are managed and financed. Agencies still work in silos, with little joint analysis or shared data, and insufficient tools, financing and capacity to manage combined climate-cyber risks.

Asia and the Pacific has the institutions and expertise to respond, but what is missing is a mindset that treats climate and cyber threats as interconnected. As climate extremes and cyberattacks accelerate, the region cannot continue fighting on two fronts with divided defences.

Building climate-cyber resilience in the region requires integrated planning, strengthened continuity systems and regional cooperation. First, joint climate-cyber assessments and exercises are needed to map interdependent failures and strengthen coordinated response. Second, critical services need strong backups, diversified connectivity and tested recovery plans that anticipate physical damage to digital infrastructure, ensuring continuity even during disasters. Third, financing and cooperation should harmonise reporting for compound events, require safeguards and build pooled insurance, supported by development banks and donors.

The convergence of climate and cyber risks is changing the nature of crises worldwide. Future disasters are likely to involve multiple, interacting shocks rather than isolated events. As this reality enters discussions in platforms such as Davos and ASEAN 2026, attention is turning to the Asia and Pacific region to advance integrated resilience as a policy priority. Delaying action will only compound impacts and put far more lives and futures at risk.

## Author/s:

**Anne Cortez**
Anne Cortez is a knowledge and communications consultant for the Asian Development Bank's climate and health portfolio. She also advises the APAC Cybersecurity Fund, an initiative of The Asia Foundation, on strategic communications and policy priorities.

Link:
https://devpolicy.org/how-do-we-navigate-asia-pacifics-climate-cyber-polycrisis-20260226/