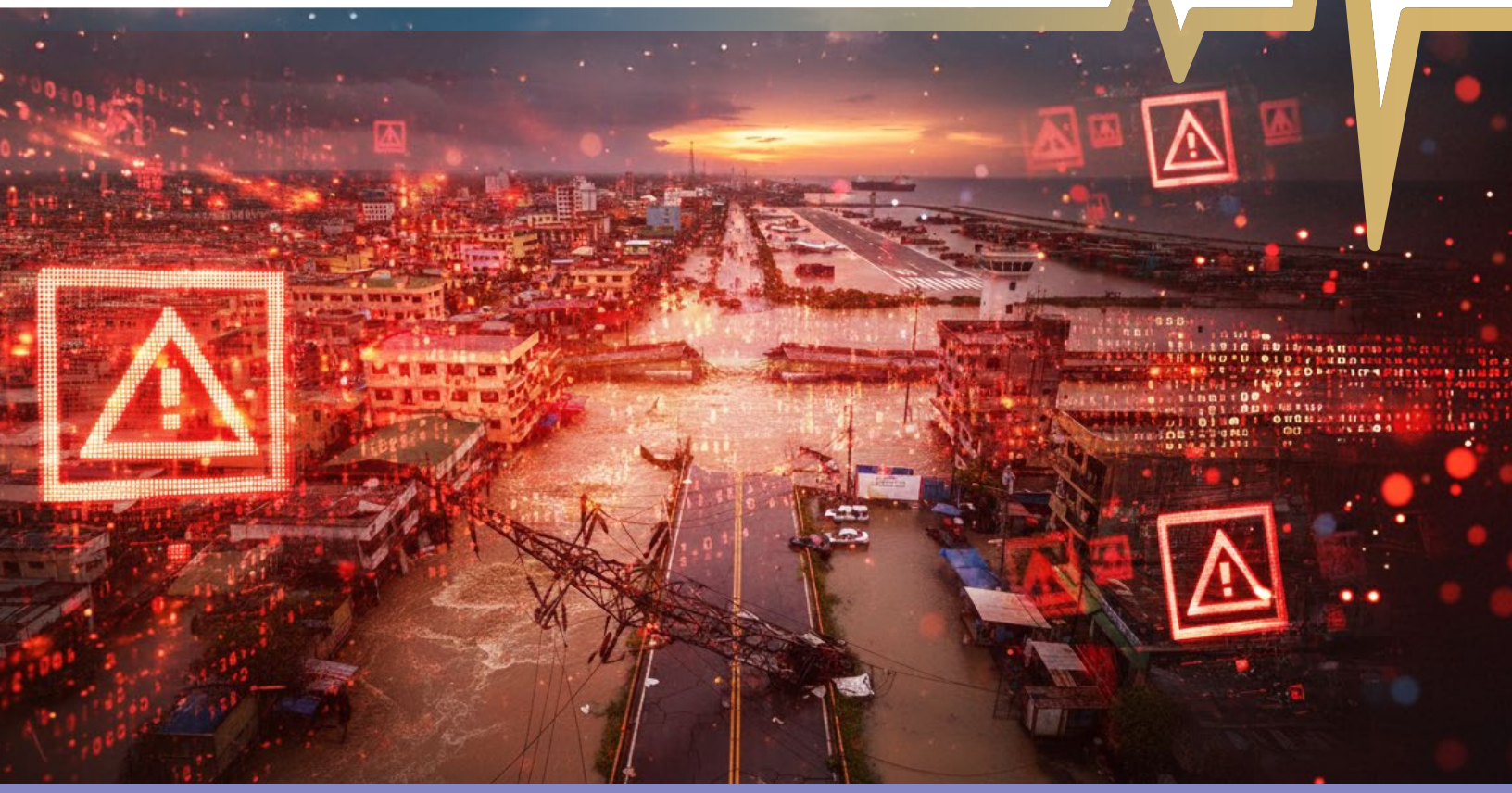
Critical Infrastructure Threat Landscape of the Philippines

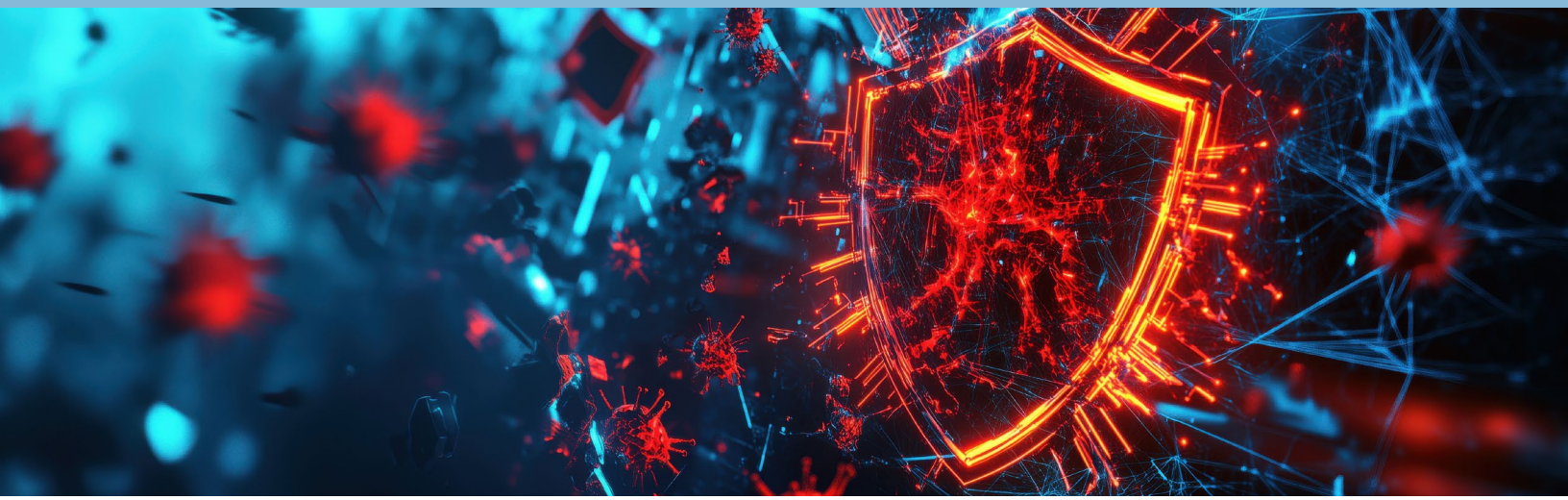
TLP:WHITE This report may be shared without restriction.



Health-ISAC®
SHARING SINCE 2010
Collaborating for Resilience in Health

health-isac.org

Contents



Key Takeaways:

- **Mass anti-corruption protests and labor strikes threaten recurring disruptions:** Large-scale mobilizations have reemerged as a destabilizing force, with peaceful demonstrations at times devolving into violence that disrupts logistics and strains emergency services. At the same time, transport unions, jeepney operators and healthcare workers have staged repeated strikes and stoppages over corruption scandals, modernization policies and unpaid allowances, creating recurring risks of supply chain bottlenecks, delayed medical services and fuel distribution interruptions.
- **Terrorism and insurgency risks remain localized but persistent:** Militant groups in the southern Philippines continue to pose episodic threats of violence and disruption to critical infrastructure, even as overall risks elsewhere in the country have declined.
- **Increasingly intense extreme weather events drive cascading threats to critical infrastructure:** Super typhoons and monsoon rains are producing more frequent power outages, road and port closures and water contamination, with unfinished or poorly maintained flood control infrastructure amplifying vulnerabilities for healthcare facilities and supply chains, while also contributing to unrest risks.
- **Chinese threat actors pose the most sophisticated cyber threats:** The most advanced cyber threats come from Chinese state-sponsored groups, which pose persistent monitoring and intellectual property theft risks, including for critical infrastructure entities, posing at least secondary threats to the healthcare sector.
- **Cybercriminals and hacktivists are becoming larger threats:** Cybercriminals and, to a lesser extent, hacktivists pose growing threats to critical infrastructure, while some nationalist hacktivist groups could escalate their activities amid flare-ups in tensions with China related to South China Sea disputes.

Mass anti-corruption protests have reemerged as a destabilizing force, periodically resulting in violent splinter actions that threaten critical infrastructure in the coming months.

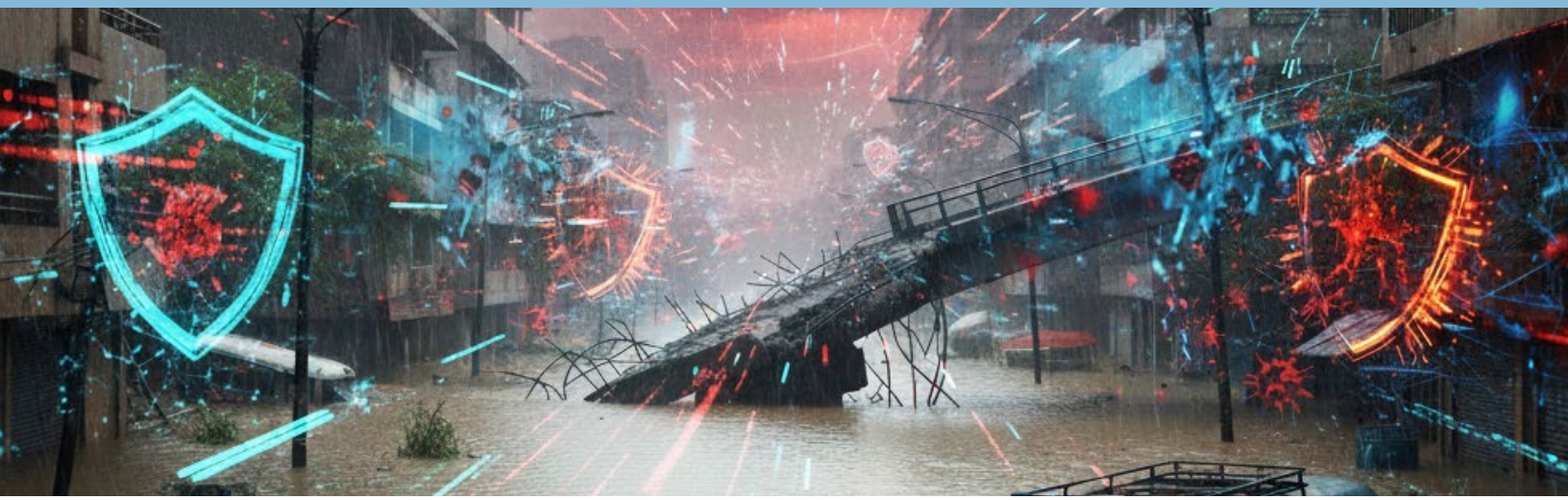
The Philippines has a robust tradition of mass protest and street mobilization, which periodically escalates into disruptive and localized violence as large, peaceful rallies at times exist in parallel with small, violent splinter actions that target symbolic sites and block transport networks. Most recently, on September 21, nationwide anti-corruption demonstrations drew nearly 50,000 people in Manila and thousands more in Cebu, Iloilo, Bacolod and Tuguegarao. The protests were driven by revelations that nearly 9,800 flood control contracts–including ghost projects, overpriced works, and substandard construction–worth $9.5 billion were paid for but never built or left unfinished, leaving communities vulnerable during Super Typhoon Ragasa and monsoon flooding earlier in the month. While the vast majority of demonstrations were peaceful, a smaller, more violent clash wherein protestors threw projectiles, including Molotov cocktails, outside Malacanang Palace – the official residence of the president – produced dozens of arrests, road blockages and property damage, as well as around 70 reported injuries to police. Looking ahead, mobilization is likely to recur over the coming months, especially around progress of investigations into the scandal, other procurement disputes and high-profile corruption prosecutions, particularly as President Ferdinand Marcos Jr. announced the formation of an interagency task force to review the contracts, ordered the Department of Public Works and Highways to conduct internal audits and referred several cases for potential prosecution. Whether these measures are seen as genuine accountability or as politicized will influence the trajectory of protest activity. Transparent proceedings and decisive indictments could help defuse public anger, but delays, weak enforcement or perceived favoritism will sustain large turnouts and increase the likelihood of further escalation, as will criticism from supporters of Vice President Sara Duterte and her father, imprisoned former President Rodrigo Duterte, who are political rivals of President Marcos Jr. and will seek to weaponize the controversy for political gain.

Labor actions across transport, public utilities and health services are a chronic operational concern for critical infrastructure.

Most recently, transport groups Manibela and PISTON initiated a nationwide strike on September 17–19, also in protest of corruption tied to flood control project misappropriations. Though the strike was cut short following pressure from commuters and government officials, the threat reflected broader volatility in the sector that also has endured repeated strikes by jeepney drivers and operators opposing the Public Utility Vehicle Modernization Program's mandated vehicle phaseouts. Healthcare workers in particular have repeatedly used walkouts, "lunch-break protests" and short stoppages to press claims over unpaid allowances, staffing shortages and hazard pay, forcing delays to elective procedures and strained emergency capacity when actions are sustained. For instance, on August 26, health workers in Mandaluyong held a lunch-break protest over longstanding unpaid allowances, staffing shortages and alleged neglect in the Department of Health. Transport sector stoppages (e.g., port, trucking and driver strikes) and government worker protests likewise have the potential to create cascading effects along supply chains that depend heavily on road freight. Given ongoing fiscal pressures, rising transport and operating costs, and public grievances over corruption and governance, the frequency and intensity of labor actions are likely to remain elevated for the foreseeable future.

Terrorism risks and resulting threats to critical infrastructure are centered on insurgent and Islamist militant groups in southern Mindanao and the Sulu archipelago.

Though Philippine security forces have degraded militant groups significantly in recent years, reducing the national-scale terror threat, resilient pockets continue to conduct kidnappings, maritime raids, and small-scale attacks that threaten coastal, port, and energy infrastructure. Multiple militant groups with differing agendas operate in the Philippines. Abu Sayyaf remains the most prominent Islamist faction, specializing in maritime kidnappings, extortion and raids; Islamic State-Philippines (ISP) and associated factions retain the capacity to conduct bombings and high-casualty urban attacks; the Bangsamoro Islamic Freedom Fighters (BIFF), a breakaway from the Moro Islamic Liberation Front (MILF), continue sporadic ambushes and improvised explosive device attacks; and communist insurgents under the New People's Army maintain a diminished but still active presence in parts of eastern and southern Luzon, Visayas and Mindanao, where they target military outposts and occasionally extort businesses. MILF itself has transitioned into the Bangsamoro Autonomous Region in Muslim Mindanao political framework in a disarmament agreement, but splinter elements remain armed. Critical infrastructure is thus an attractive though indirect target. Militants typically focus on soft targets such as villages, ferries or remote installations, but attacks can spill over to ports, power facilities or transport corridors. Joint U.S.-Philippine deployments in the Sulu region reflect ongoing concerns that militant factions could disrupt regional energy projects, coastal shipping lanes or humanitarian relief operations during storm season. As such, episodic, localized disruptions, armed extortion, maritime kidnappings affecting supply chains and IED attacks that delay ground transport or deter contractors remain risks to monitor. While improved counter-terrorism capacity in recent years reduces the likelihood of sustained large-scale assaults, these groups' continued presence underscores that insurgent violence will remain an enduring background risk in the Philippines, especially as the Philippines' strategic reorientation toward countering Chinese threats in the South China Sea risks diverting personnel, budgets and political attention.



The Philippines' exposure to tropical cyclones, heavy monsoon rainfall and related floods and landslides represents one of the most consequential and recurring risks to critical infrastructure, with storms increasingly intense due to climate change and rapid urbanization in coastal areas.

The Philippines' geographic position within the main typhoon belt of the Pacific Ring of Fire puts it at high risk for a variety of natural disasters. These hazards can overwhelm power transmission lines, inundate roads and bridges, damage airports and ports, and compromise water treatment facilities, producing cascading failures that interrupt electricity, transport and medical supply chains for days at a time. While disaster agencies have improved forecasting and evacuation protocols, rapid urbanization, inadequate drainage and aging assets leave densely populated and coastal areas especially vulnerable. Storms can force port closures, delay medical imports, disable hospital power systems (even with generators) and drive surges in demand that strain already limited emergency services. Looking ahead, the increasing intensity of tropical cyclones linked to climate change, coupled with population growth in flood-prone areas, ensures that extreme weather will remain a structural risk.

Super Typhoon Ragasa in September forced mass evacuations, toppled transmission lines in northern Luzon and suspended work and classes across Metro Manila. This storm is directly linked to recent protest activity as flood-control mechanisms tied to nearly 9,800 contracts worth $9.5 billion were either unfinished or never built, leaving communities exposed to severe flooding and fueling public anger over corruption.

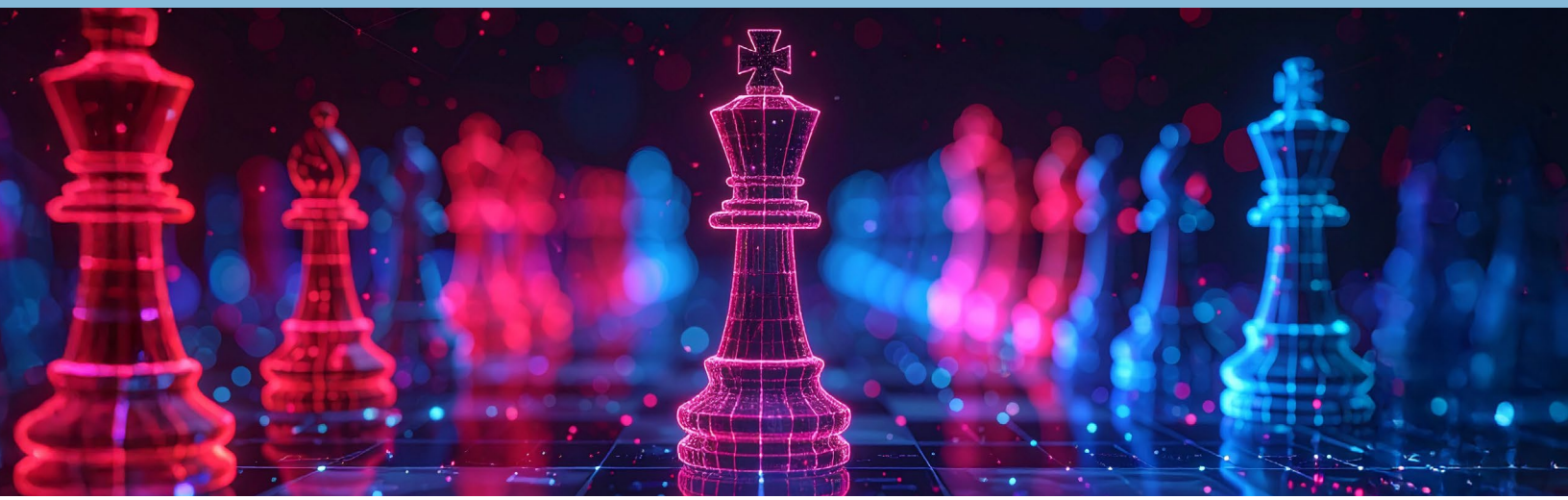
Chinese state-sponsored groups are the most sophisticated cyber threats to Philippine cyberspace and routinely target sensitive networks, including critical infrastructure, for cyberespionage, persistent monitoring and data theft, posing at least secondary risks for healthcare entities.

In tandem with rising maritime and military tensions with China, Chinese cyber threat activity targeting the Philippines has also risen. In line with Beijing's broader aggressive pace of offensive cyberespionage campaigns, Chinese advanced persistent threat (APT) groups have repeatedly breached Philippine networks, with a special emphasis on entities linked to the countries' maritime disputes. These persistent monitoring campaigns have exposed sensitive Philippine databases and internal systems to spying, as well as data exfiltration and intellectual property theft. Although there is no clear precedent for Chinese threat actors pursuing more disruptive cyberattacks against Philippine targets, Beijing possesses toolkits capable of causing disruption and likely leverages at least some co-opted networks to preposition malware, especially given Manila's defense alliance with Washington. All the same, these campaigns have generally stayed confined to more strategic political and military targets and, as such, the direct risk posed to healthcare entities is likely comparatively much lower. Still, given Chinese APTs' tendencies to breach software supply chains, they have likely accessed some organizations in the healthcare sector. Beijing's long precedent of aggressive intellectual property theft means that any breached organization could be at risk of losing critical information or, if their networks are not well secured, further lateral compromise that impacts other parts of a company. While the Philippines has also witnessed a significant uptick in hacktivist campaigns, there have been no clear attributions that any of these groups have direct ties to the Chinese government. It can be presumed that at least some hacktivism is spurred by Chinese threat actors, with many observed hacktivists being homegrown actors, discontented with the government's policies or performing direct retaliatory actions against perceived Chinese threats. Thus far, these campaigns have only involved limited website outages or defacements, with healthcare entities unlikely to be immediate targets.

On January 20, Philippine authorities arrested a Chinese national along with two Filipino nationals accused of using surveillance equipment to spy on critical infrastructure, including military facilities, while operating under the guise of working as autonomous vehicle developers. In total, six people were accused of being involved in the operation, three of whom resided in China and one who maintained ties to a university under the control of the People's Liberation Army. By mid-April, Philippine authorities arrested at least a dozen Chinese nationals on similar charges.

On January 6, Bloomberg reported that for over a year the Chinese group APT41 had maintained access to swaths of internal networks linked to the Philippines' executive branch and stolen data from agencies associated with coastal defense, including documents on Chinese-Philippine territorial disputes in the South China Sea.

In 2024, Philippine-based threat actors, primarily hacktivists, initiated a campaign known as #OpChina, targeting Chinese entities including government, hospitals, and educational institutions in a counter-response to rising tensions in the South China Sea.



The Philippines is facing growing cybercriminal threats, with certain tactics, such as ransomware targeting critical infrastructure entities, most likely to result in operational disruptions to key processes and services, while other types of attacks primarily threaten financial losses.

Amid growing ransomware threats in the region alongside the country's weak enforcement of cybersecurity laws and outdated infrastructure, organizations face a heightened risk of disruptions and financial losses, with attacks targeting critical infrastructure more likely to cause disruptions to key services. Critical infrastructure entities are also more likely to be targeted as threat actors believe that the critical nature of their services mean that victims will be more likely to pay ransom to avoid lasting disruptions. Beyond increasing ransomware threats in recent years, Chinese cybercriminal groups have also become increasingly prevalent in the Philippines, with the country now regarded as one of the most heavily targeted countries in the region. In particular, China-based cybercriminal groups have increasingly carried out smishing campaigns in the Philippines to steal large volumes of compromised payment data, with Chinese cybercriminal groups on the dark web and Telegram channels often revealing the Philippines as having the highest volumes of compromised credit cards. There is also a growing presence of cyber-scam compounds in the country, or hubs housing operations for large-scale cyber frauds. These centers are often run by Chinese or transnational criminal gangs and carry out scams against both foreign and domestic targets, with an increased presence in the Philippines inherently resulting in an uptick in fraud operations, like crypto or romance scams, locally. These international threat groups, which hire Filipino scam agents, have been observed using International Mobile Subscriber Identity (IMSI-Catcher) devices to intercept mobile phone traffic and track device locations. The scam operators move around highly-transited areas, like downtown Manila, to send smishing messages to intercepted devices. Furthermore, criminal gangs recruit forced labor for the scam compounds through fraudulent job postings online offering high salaries for roles like customer sales representatives or chat support agents before individuals are trafficked to either local compounds or those in nearby countries like Myanmar, Laos or Cambodia.

74%

According to a July 2025 report from U.S. cybersecurity firm Resecurity, 74% of Filipinos **reported being recently targeted with email, phone call or text messaging scams.**

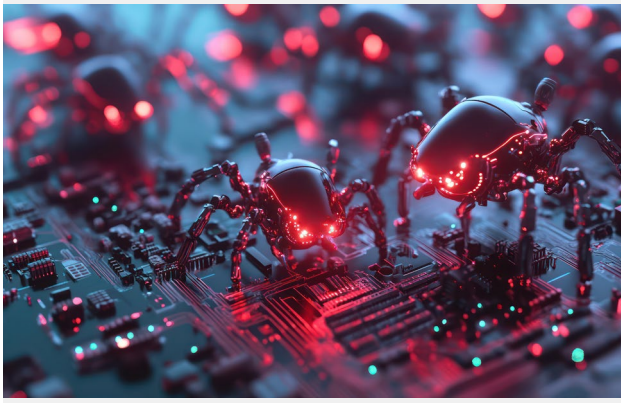
1 in 4

According to a May 2025 report from the Inquirer, citing sources from U.S. cybersecurity firm Fortinet, one in every four companies in the Philippines has **paid over $500,000 to recover** from a ransomware attack.

Politically-motivated hacktivists are also increasingly active, with most activity resulting in low-level, temporary disruptions, such as website defacements and distributed-denial-of-service (DDoS) attacks, though data theft and ransomware deployment remain risks.

The Philippines has a highly active hacktivist threat landscape, with a wide array of groups engaging in activities to protest the Philippine government or engage in international activism. Groups like Philippine Cyber Alliance, Bisaya Cyber Army, and Nullsec Philippines typically engage in website defacement and DDoS attacks to largely express anti-corruption, anti-censorship or anti-authoritarian grievances, with such attacks only causing small-scale, short disruptions. However, the country's most sophisticated domestic threat actor, DeathNote Hackers, has been observed pivoting from hacktivism to bug bounty activities, even as other sophisticated groups like Ikaruz Red Team have been documented using ransomware, and groups like Exodus Security and the #opEDSA campaign have leveraged other methods to exfiltrate data. The attacks targeted Philippine entities and shared similar anti-authoritarian motivations as other notable hacktivist groups. Many of these sophisticated groups also express support for state sovereignty and include either explicit or implicit anti-China sentiments or undertones in their messaging. This means that these groups could elevate their activities amid flare-ups in bilateral tensions, such as over South China Sea disputes, targeting Chinese entities or potentially even Philippine entities in protest of government or private sector actions, heightening risks of data theft or potentially of ransomware attacks and subsequent operational disruptions. Moreover, the Philippines' Department of Information and Communications on September 22 warned that a group called Black Mask March with ties to Anonymous PH, which carried out protests against China in 2014, is linked to anti-government protests in Manila which began on September 21. The warning states that the groups' online calls to action resulted in violent street demonstrations and said that the group had also carried out 1.4 million breach attempts and DDoS attacks amid the protest campaign, illustrating how hacktivist groups can also facilitate physical threats.

In February 2025, Exodus Security claimed to have breached the systems of the Philippine Army and Navy and accessed roughly 10,000 records of active and retired military personnel. The same month, the group also claimed to have obtained sensitive personal information of lotto winners from 2016–2025 from a breach of the Philippine Charity Sweepstakes Office.



In March and April 2024, threat actor Ph1ns claimed to breach and exfiltrate, and in some cases delete, data from the Philippine Department of Science and Technology, third party Philippines vendor Acer Philippines and firms owned by then-Philippine House of Representatives Speaker Martin Romualdez, including Prime Media Holding, Marcventures Holdings and Bright Kindle Resources.

Conclusion

Health Sector Analyst Takeaway

Tensions with China manifest as direct threats to local critical infrastructure, implicating the health sector in geopolitical conflicts. Filipino threat actors have expressed anti-China sentiment during their attacks. Considering the recent action of the Chinese government has designated the disputed Scarborough Shoal area as a maritime nature reserve, the fallout may lead to increased cybercrime as tensions between the Philippines and China escalate.

From a physical security perspective, the large protests raise concerns for operational resilience. The protests could block critical emergency medical service (EMS) routes and force ambulances to take alternative routes. They also could raise political concerns which may be reflected in hacktivist activities against Filipino critical infrastructure, placing local health sector organizations. Extreme weather events can also impact critical infrastructure access by making roads inaccessible and causing sudden power outages.

Members in the Philippines are encouraged to host scenario-based risk planning exercises that cover major cyber attacks, natural disasters and large scale protests to form resilience plans. Some actionable steps that members can take to shore up possible cybersecurity vulnerabilities include mandated multi-factor authentication on all patient data portals and requiring users to change their passwords once every 90 days.

More Health-ISAC® whitepapers can be found here: https://health-isac.org/post-type/white-papers/

Feedback on this white paper and suggestions for future topics are encouraged and welcome. Please email us at contact@h-isac.org.