

China introduces emergency cybersecurity plan

China released Tuesday an emergency response plan for Internet security incidents.

The plan was formulated and released by the Office of the Central Leading Group for Cyberspace Affairs, to “improve handling of cybersecurity incidents, prevent and reduce damage, protect the public interest and safeguard national security, public safety and social order.”

The plan divides cybersecurity incidents into six categories, including pernicious procedural incidents, cyber attacks and information security incidents.

It also defines four-levels of security warnings and response systems according to threat conditions ranging from “general” to “extremely serious.”

Under the top “extremely serious” condition, security incidents may “paralyse many important Internet and information systems and halt operations,” or “cause loss or falsification of state secrets and important sensitive information, posing great threats to national security and social stability,” according to the plan.

Serious incidents will trigger measures including establishment of emergency headquarters, 24-hour monitoring and multi-department coordination in handling the aftermath.

In May, China suffered from a global ransomware attack that had paralyzed online payment systems at petrol stations across China and invaded colleges to encrypt papers and other documents.

The plan is also an implementation of the Cybersecurity Law adopted last year, which requires an emergency response mechanism from cyberspace authorities to avoid such threats.

Authorities are asked to organize rehearsals and strengthen prevention, especially during important meetings or national events.

Those who fail to implement the measures or conceal cybersecurity incidents will be punished, according to the plan.