The three-year NoAH project gathers and analyses information about the nature of Internet cyberattacks. NoAH designs and develops an infrastructure for computer security monitoring based on honeypot technology.

Honeypots are computer systems that are intentionally made to appear vulnerable and closely monitored to analyse attacks directed at them. NoAH integrates geographically-dispersed honeypots as an early-warning system, and correlates the received data to generate warnings and possibly trigger appropriate containment measures.

The aim is to help NRENs (National Research and Education Networks) and ISPs (Internet Service Providers) limit damage to their networks, allow information security organisations to better assess threats, and provide researchers with a wealth of attack-related data to improve detection techniques.