NUS National University of Singapore | ISAS Institute of South Asian Studies

ISAS Brief

No. 965 – 27 September 2022

Remedying Ransomware: The Quad's Manifest Cyber Agenda

Karthik Nachiappan

Summary

The Quadrilateral Security Dialogue's entry into functional issue areas, specifically critical technologies, finds shape and possible momentum with a focus on preventing ransomware attacks across the Indo-Pacific.

In June 2022, the Quadrilateral Security Dialogue (Quad) unveiled an expanded agenda where the four countries – Australia, India, Japan and the United States – could work together in specific working groups to achieve objectives in functional issues like climate change, health and critical technologies. These groups have had additional meetings since their announcement. The impetus to drive momentum and achieve greater convergence appears to be imminent on technology and digital issues. This past week, the Quad's foreign ministers released a joint statement on cyber-attacks that represents an important development to tackle the rising spate of threats online. The scope and potential of these Quad cyber discussions remain to be seen. Still, the prospects of meaningfully addressing such threats become greater when these conversations sustain and extend to how each Quad country advances these objectives bilaterally and multilaterally.

The Quad's working group on emerging technologies was created with the recognition and motivation that a need existed to develop, govern and operate technologies out of shared values and interests. The increasing use and misuse of technologies by states and state actors precipitated a need to establish new standards and rules that could govern and manage the effects of technologies across countries. Arguably implicit in this framing, the Quad's technology agenda is the mutual concern of all four countries with China – how Beijing seeks to use technologies for domestic purposes and how those strategies affect the interest of the Quad and other countries. This mandate converges with cybersecurity through the need for new rules and frameworks and to share information on contingent threats online to boost domestic defences and preparedness. The recently released statement on ransomware attacks testifies to this reality.

The Quad's joint statement on ransomware, issued after the four foreign ministers met at the United Nations (UN) General Assembly in New York, targets state-sponsored malicious cyber activities emanating from China, Russia and Iran that target critical infrastructures across the Quad countries. The statement also identifies and singles out ransomware attacks, a type of attack where the source locks and encrypts the victim's data and critical files and expects payment to unlock and decrypt data. One recent cybersecurity firm identified ransomware attacks as the number one threat to large and medium-sized businesses, including government organisations, in 2022. Ransomware attacks have also increased as users and businesses' reliance on the cloud increases, allowing hackers to focus their attention on cloud-based networks. Cybercriminals rely on ransomware attacks that exploit existing software vulnerabilities to extract data. The rising public use of more recent technologies like cryptocurrency and decentralised finance systems has expanded the options criminals have in deploying ransomware.

The Quad's statement on ransomware is welcomed, given the rising spate of malware attacks globally, particularly from the three countries identified in the statement – China, Russia and Iran. Moreover, the statement notes the 'transnational nature' of ransomware, given the difficulties inherent in locating the source while being clear that its effects are not purely security based but also extend to the economy, especially the financial and industrial sectors. The Quad's statement also promised future cooperation on ransomware to ensure their cyber infrastructures remain strong and resilient as ransomware attacks increase. Critical infrastructures are a particular concern, especially in sectors like finance and health, where data remains sensitive. Indeed, the lack of effective data protection frameworks in some Quad countries, notably India, raises the costs and implications of ransomware attacks that imperil the personal data of millions. Ransomware appears to be a call to action for the Quad's critical technologies working group.

Besides cooperation through the Quad, each Quad member also signalled its desire to extend incumbent conversations and progress to support and advance prevailing global cybersecurity mechanisms and frameworks, specifically the UN Framework for Responsible State Behaviour in Cyberspace, Global Forum on Cyber Expertise and a potential UN Framework Convention on Cyber Crime. Broadly, the Quad's cyber initiatives must cohere with and advance existing multi-stakeholder approaches to internet governance, whose principles work to protect the internet's sanctity through governance mechanisms that are inclusive and broad-based.

Yet, it is perhaps worth remembering that each Quad member's domestic cybersecurity situation appears distinct, affecting the scope of cooperation on this issue. That India lags its Quad counterparts on cyber defences and preparedness does not spell doom, but it could constrain the speed at which they could collectively respond to ransomware attacks. That the Quad's statement pledges to also foster cooperation on cyber capacity building through initiatives aimed at enhancing regional cybersecurity and improving resilience against ransomware attacks in the Indo-Pacific appears to be a promising development. Training aside, it is vital for the Quad countries to identify how to best quantify progress on ransomware defence and deterrence. In other words, what practical measures will or can the Quad countries take to counter ransomware but also prevent specific countries from becoming safe havens to ransomware actors? Fundamentally, strengthening cyber resilience across the Indo-Pacific will hinge on this latter objective.

. . . . .

Dr Karthik Nachiappan is a Research Fellow at the Institute of South Asian Studies (ISAS), an autonomous research institute at the National University of Singapore (NUS). He can be contacted at isaskn@nus.edu.sg.
The author bears full responsibility for the facts cited and opinions expressed in this paper.