**Cyberspace policy**

Areesha Anwer

Thursday, Mar 17, 2022

According to the Identity Theft Resource Centre (2021), the total number of data breaches in 2021 was 1,291 compared to 1,108 breaches in 2020. Cyber security experts estimate that by 2025 global cybercrimes would cost $10.5 trillion annually. This requires states to adopt robust and efficient strategies and maintain effective deterrence to mitigate cyber-related threats.

The threat of a Cyber Pearl Harbor can be traced back to the World Wide Web’s (WWW) prominence since the 1990s. Sean Lawson and Michael K. Middleton (2019) explain Cyber Pearl Harbor as “catastrophic physical impacts from cyber-attacks on critical infrastructure.” Terminologies such as ‘cyberwars’, ‘cyber-attacks’, and ‘cyber-intrusions’ have diffused into the discourse of state security as they threaten countries with novel aspects of warfare. Having said that, a Cyber Pearl Harbor as of yet remains hypothetical. However, low-stakes cyber operations involving states and non-state actors, as well as high-stakes cyber operations among big powers are carried out frequently.

Cyber-attacks are central to high-level diplomatic discussions as states view them as a matter of national security. During a summit held between President Biden and President Putin in Geneva on June 16, 2021, the US president gave a list of sixteen US critical infrastructure to President Putin that should be off-limits to cyber-attacks. The list included sectors such as energy, nuclear reactors, healthcare, chemical, IT, and the defence industrial sector. The summit signaled US’s national security concerns as well as its vulnerability, as this interaction came immediately after a massive cyber-attack on the Colonial Pipeline in May 2021.

Establishing deterrence in cyberspace remains a challenge. Joseph Nye in his article ‘Deterrence and Dissuasion in Cyberspace’ explains that since deterrence by punishment depends on attribution as both states and non-state actors have access to cyber weapons, deterrence by denial will work more effectively. To prove his argument, he refers to an example of a cyber-attack on the JPMorgan Chase bank in 2012, which resulted in the compromise of Personally Identifiable Information (PII) of 76 million households and seven million businesses. The attack was widely linked to Russia. However, in 2015 the US Justice Department identified the attackers to be a sophisticated criminal gang led by two Israelis and a US citizen.

In addition, the problem of attribution in cyberspace also leads to blame-game among states. For example, the US accused China of the Microsoft Exchange hack in 2021 and China has criticised the US for being “the world’s largest source of cyber-attacks.” Likewise, Western countries use phrases such as ‘highly likely’ to accuse their adversaries of cyber-attacks without having concrete evidence.

This indeed points to ambiguity when it comes to attribution and thus states fall back on deterrence by denial. An important question for policymakers is whether deterrence by denial is effective on its own. Maintaining good cyber hygiene and robust cyber-infrastructure may be effective in guarding off cyber-attacks by states or non-state actors. However, this does not entirely eliminate the possibility of cyber-attacks.

Pakistan ranks 79th in the Global Cybersecurity Index. However, in the global trend of cyber-attacks, Pakistan is no exception. For instance, some recent major cyber incidents in Pakistan have been directed towards banking and energy infrastructures. These include K-Electric, the Federal Board of Revenue (FBR), and the National Bank of Pakistan (NBP). Moreover, there have also been reports of cyber espionage by foreign security agencies. It was also reported by ISPR in 2020 that Indian intelligence agencies were involved in cybercrimes against government officials and military personnel in Pakistan.

In the same context, a 2021 report by Amnesty International highlighted that Pegasus spyware was used by India against Pakistan. A related article published by Global Times in November last year highlighted how a hacker group based in India launched cyber-attacks on government and security departments in Pakistan and China.

Pakistan’s National Cybersecurity Policy 2021 mentions taking retaliatory measures in case of aggression on Pakistan’s critical infrastructure. Its objective states that ‘[It] Will regard a cyber-attack on Pakistan CI/ CII as an act of aggression against national sovereignty and will defend itself with appropriate response measures.’ However, the deterrence mechanism mainly followed by the policy is deterrence by denial – denying any benefit to the attacker. This does not maintain a complete cyber deterrence.

An asymmetric cyber-attack may require adequate defence, but to deter a large-scale symmetric cyber-attack, cyber defense coupled with non-cyber means of retaliation would maintain an effective deterrence. Hence, states have incorporated retaliatory measures in their cyber-security policies and nuclear doctrines. For instance, the US Department of Defense 2018 Cyber Strategy is offensive in nature and states the development of a lethal joint force for countering malicious cyber actors.

According to a recent statement by Pakistan’s leadership, Pakistan’s IT exports are expected to reach $50 billion within the next few years. This is certainly a path to a resilient digital infrastructure. However, to defend the cyber frontiers, earnest implementation of the cyber-security policy will be helpful in deterring cyber-attacks.

Maintaining deterrence in cyberspace is an uphill task, yet not impossible. Strong cyber-security infrastructure is integral to minimising cyber vulnerabilities. Alongside policy implementation and strengthening the regulatory mechanism, further investments in emerging technologies must be made. This will help augment cyber defence, create an effective deterrence posture, and enhance the indigenous cyber capability of Pakistan.

The writer is a research officer at the Center for International Strategic Studies Sindh (CISSS).