Response to cyber attacks

What is the issue?

\n\n

Publicly attributing the cyber attacks to a state or non-state actor is vital for building a credible cyber deterrence strategy.

\n\n

What are the recent incidents?

\n\n

\n
- The US Department of Justice filed a criminal complaint in September indicting North Korean hacker Park Jin Hyok for playing a role in at least three massive cyber operations against the US.
\n
- This included the Sony data breach of 2014, the Bangladesh bank heist of 2016 and the WannaCry ransomware attack in 2017.
\n
- This indictment was followed by another complaint on Russia’s military agency for persistent and sophisticated computer intrusions in U.S.
\n
- Evidence adduced in support included forensic cyber evidence like similarities in lines of code or analysis of malware and other factual details regarding the relationship between the employers of the indicted individuals and the state in question.
\n
- The above criminal complaints will not necessarily lead to the prosecution of the indicted individuals across borders.
\n
- However, indicting individuals responsible for cyber attacks is in itself an attractive option for states looking to develop a credible cyber deterrence strategy.
\n

\n\n

What is the importance of attributing cyber attacks?

\n\n

\n
- There are technical uncertainties in attributing attacks to a specific actor.
\n
- It has long fettered states from adopting defensive or offensive measures in response to an attack and garnering support from multilateral fora.
\n
- Cyber attacks are multi-stage, multi-step and multi-jurisdictional, which complicates the attribution process and removes the attacker from the infected networks.
\n
- Experts have argued that technical challenges to attribution should not detract from international efforts to adopt a robust, integrated and multi-disciplinary approach to attribution.
\n
- It should be seen as a political process operating in symbiosis with technical efforts.
\n
- A victim state must communicate its findings and supporting evidence to the attacking state in a bid to apply political pressure.
\n
- Clear publication of the attribution process becomes crucial as it furthers public credibility in investigating authorities.
\n
- It enables information exchange among security researchers and fosters deterrence by the adversary and potential adversaries.
\n
- Also, a criminal indictment is more legitimate as it needs to comply with the rigorous legal and evidentiary standards required by the country’s legal system.
\n
- Further, an indictment allows for the attack to be conceptualised as a violation of the rule of law in addition to being a geopolitical threat vector.
\n

\n\n

What are the lessons for India?

\n\n

\n
- India is yet to publicly attribute a cyber attack to any state or non-state actor.
\n

- This is despite an overwhelming percentage of attacks on Indian websites perpetrated by foreign states or non-state actors, with 35% of attacks emanating from China, as per a report by CERT-IN.
\n
- Along with the National Critical Information Protection Centre (NCIIPC), CERT-IN forms part of an ecosystem of nodal agencies designed to guarantee national cyber security.
\n
- There are three key lessons that policy makers involved in this ecosystem can take away from the WannaCry attribution process and the Park indictment.
\n
- First, there is a need for **multi-stakeholder collaboration** through sharing of research, joint investigations and combined vulnerability identification among the various actors employed by the government, law enforcement authorities and private cyber security firms.
\n
- Second, the standards of attribution need to **demonstrate compliance** both with the evidentiary requirements of Indian criminal law and the requirements in the International Law on State Responsibility.
\n
- The latter requires an attribution to demonstrate that a state had 'effective control' over the non-state actor.
\n
- Finally, the attribution must be **communicated to the adversary** in a manner that does not risk military escalation.
\n
- Improving attribution capabilities is as equally important as building capacity to improving resilience and detecting cyber attacks.
\n
- Thus India will need to marry its improved capacity with strategic geopolitical posturing.
\n
- Lengthy indictments may not deter all potential adversaries but may be a tool in fostering a culture of accountability in cyberspace.
\n

\n\n

\n\n

Source: Business Line

\n

SHANKAR
IAS PARLIAMENT
Information is Empowering