The new front

In October 2014, the US Department of Defense constituted a task force under the Defense Science Board to “consider the requirements for effective deterrence of cyber attacks”. The report, submitted in February 2107, has this to say in its introduction: “The unfortunate reality is that, for at least the next decade, the offensive cyber capabilities of our most capable adversaries are likely to far exceed the United States’ capability to defend key critical infrastructure.”

Coming from a country which is today the best prepared to deal with all aspects of cyber warfare, this statement should serve as a grim reminder of the seriousness of this threat. As “Digital India” grows, vulnerabilities will only increase. A 2017 study conducted by Symantec found that India ranked fourth in online security breaches, accounting for over 5 per cent of global threat detections.

Cyber threats can manifest in many ways but what is visible on an almost daily basis are cyber crimes, cyber theft, cyber espionage, cyber intrusions etc. These are relatively low-end threats but seem to occupy all our attention. It is for this reason that we hear official statements about how initiatives like the National Critical Information Infrastructure Protection Centre (NCIIPC) and the appointment of a National Cyber Security Coordinator have improved our ability to deal with cyber attacks. This is only the tip of the iceberg and is lulling us into a false sense of complacency.

Criminal hackers can certainly cause data breaches and financial loss, and countering them is important, but these are not attacks which threaten the security of a country. The real danger to India lies in targeted cyber attacks coming from adversarial nation states. Countries like China can bring immense assets to bear in carrying out sophisticated cyber attacks. The success of Stuxnet, which damaged the Iranian centrifuge facility at Natanz, lay in the fact that it was an international operation involving the CIA, NSA and Israel’s Unit 8200. The highly sophisticated malware used an unprecedented five zero-day exploits and was tested on a dummy set of centrifuges built for this purpose. Such capability is not available with groups of hackers.

If, and it appears increasingly likely, cyber warfare is going to become a regular part of the arsenal of nations, there is a need to visualise how this war will be fought and under whose responsibility. Let me attempt to decode this briefly.

The three main components of any national strategy to counter cyber threats are defence, deterrence and exploitation. Critical cyber infrastructure needs to be defended and the establishment of the NCIIPC is a good step in this direction but individual ministries and private companies must also put procedures in place to honestly report breaches. It is only then that the NCIIPC can provide the requisite tools to secure these networks. This partnership must be transparent and not mired in the usual secrecy of intelligence organisations.

However, as brought out at the beginning of this article, there are limits to defending as the dice are loaded in favour of offensive capabilities. Therefore, deterrence and exploitation become critically important. Deterrence in cyberspace is a hugely complex issue. Nuclear deterrence worked because there was clarity on the capability of adversaries and the horrific cost of a nuclear conflict. Cyber warfare is characterised by an absence of clarity. We can never be certain about the capability of the other side (there are no missiles to be counted) and also the chances of success if we launch a cyber counterstrike.

It is for these reasons that deterrence cannot be limited only to the cyberspace. The 2017 Defense Science Board report, in talking about “deterrence by cost imposition”, states, “While offensive cyber responses are an essential part of the toolkit, the full range of military responses (symmetric

or asymmetric) — as well as diplomatic, law enforcement and economic responses — must also be considered."

And finally, the exploitation of cyberspace to achieve national security objectives. Again, cyber operations cannot be a standalone activity but integrated with land, sea and air operations, and a part of information warfare. The preparation for this will have to start with the Indian military gathering intelligence, evaluating targets and preparing the specific tools for cyber attacks. This will then be meshed with the war-fighting plans of the three services.

Looked at in its entirety, the most serious manifestation of cyber attacks is when an external state threatens the national security of India by exploiting the cyberspace. If this is clear, then the danger cannot be countered by an intelligence agency like the NTRO or a research organisation like the DRDO. The lead agency to deal with this will have to be the defence services, which are responsible for protecting India. It is here that we are completely ill-prepared.

India is one of the few countries which still does not have a dedicated cyber component in its military. The setting up of a Defence Cyber Agency has been announced but this is a typical half-hearted step which characterises our strategic planning process. The upgrading of this agency to a Cyber Command must be implemented at the soonest.

What will also be important is the authority and mandate given to the Cyber Agency. If it is hobbled by limited mandates and roles, as often happens due to inter-agency rivalries, India will never achieve the full capability of fighting and defending in the cyberspace. It would be instructive to take a leaf out of the US Cyber Command, which has one of its focus areas as "strengthening (the) nation's ability to withstand and respond to cyber attack".

In 2012, US Defense Secretary Leon E Panetta warned that the country was facing the possibility of a "cyber-Pearl Harbor". Many strategic experts like Martin Libicki, Joseph Nye and Thomas Rid have argued that the fears of such catastrophic cyber attacks are overblown. We are still unclear about how a future cyber war will play out but capabilities definitely exist, particularly with China. It would be absurd not to prepare, and the military must be at the forefront of this preparation.

END