The wings of Pegasus, the epoch of cyberweapons

With their use not only during a conflict but even during peacetime, matters have reached a tipping point

M.K. NARAYANAN

A raging controversy across the world on the misuse of Pegasus spyware – a great deal of which is mired in facts, suppositions, false trails, allegations and counter-allegations, but nevertheless contains more than a kernel of truth – has reignited a debate on the role of cyber weapons. From an occasional and sporadic instance of a cyberattack previously, cyberattacks on institutions such as banks and on critical infrastructure have proliferated to an alarming extent, signalling the emergence of the cyber weapon epoch.

The Pegasus spyware is by no means the ultimate cyberweapon. It has, however, compelled nations to emerge from their deep slumber about the threat posed by such new age weapons, even though it has been quite a few decades since the world saw the advent of cyberweapons, albeit more primitive than those in vogue today.

An evolution

One of the earliest instances of this kind occurred in the 1990s when Yahya Abd-al-Latif Ayyash, who served as the chief bomb maker for Hamas, was assassinated by Israel's domestic Intelligence Agency, Shin Bet, using a doctored phone containing explosives, when he responded to a call from an unknown person. Many daring exploits of the past, which took months of effort, and the utilisation of large numbers of people and resources to achieve, are, in the cyber era, possible with far less effort and resources; the destruction of the Vemork power station (in Norway) during the Second World War which took months of planning, and the extensive resources of the Allied Powers (and involved loss of lives), for instance, could be achieved in 2019 with a fraction of this effort. In 2019, Norsk Hydro, aluminium and energy producer, became the victim of a cyberattack which was accomplished remotely and anonymously, and in the shortest possible time, but with the same telling effort.

What is noteworthy is that while all of these rate as among the many dramatic transformations brought about by cyber technologies since the turn of the century, what merits contemplation is that while Moore's Law democratised access to computing, and the Internet opened a whole new avenue for communication, all this is coming at a price. Privacy has been eroded and the Internet – true to its origins in Cold War strategy – has become a powerful weapon in the hands of those seeking to exploit its various facets.

Now, a preferred weapon

Cyber is often touted as the fifth dimension of warfare – in addition to land, sea, air and space. However, it needs to be understood that cyber, as the domain of military and national security, also co-exists with cyber as a domain of everyday life. It is the same domain. The war is no longer out there. It is now directly inside one's drawing room, with cyberweapons becoming the weapon of choice.

Israelis, though not the cyber pioneers, today dominate the cyber domain along with the Chinese, Russians, Koreans and, of course, the Americans. Already by the first decade of the 21st century, cyberspace had graduated from being merely the new domain of warfare, into becoming fundamentally a civilian space. From its very inception, cyberweapons ranked as special weapons, not unlike nuclear devices of earlier times. Following the joint U.S.-Israeli effort in unleashing the Stuxnet Worm in 2010 – which helped disable several hundred centrifuges at the Iranian nuclear facility in Natanz – it became still more apparent that mankind had indeed unleashed a new weapon, and had in a sense crossed the Rubicon.

The linkage between sabotage and intrusive surveillance is but a short step. There are many stories in circulation of the employment of the Pegasus spyware well before the present controversy, for in

GETTY IMAGES/ISTOCKPHOTO

2019, WhatsApp had sued NSO over allegations that several hundreds of its users were the targets of the Pegasus spyware. The Israeli company's claim that the spyware is sold only to governments and official agencies is, however, unproven. Israel, for its part, identifies Pegasus as a cyberweapon, and claims that its exports are controlled.

Work in progress

The Pegasus spyware it is stated can copy messages that are sent or received, 'harvest photos and record calls, secretly film through the phone's camera, or activate the microphone to record conversations. It can potentially pinpoint where you are, where you have been, and whom you have met. Once installed on a phone, the spyware can harvest more or less any information or extract any file'. Ongoing efforts by the NSO Group, the makers of Pegasus, are devoted to making the spyware difficult to detect.

An earlier version of Pegasus, identified as far back as 2016, infected phones mainly through 'spearphishing'. Since then, its capabilities have vastly increased, and it currently employs 'zero click' attacks, which do not require any interaction on the part of the phone owner. It is used to exploit certain 'zero day' vulnerabilities found in operating systems – about which the manufacturers themselves are unaware. Where 'spearphishing' or a 'zero click' attack cannot succeed, the Pegasus spyware can be installed over a wireless trans-receiver located near a target. Essentially, the Pegasus virus seeks what are termed as 'root privileges' – that enable communication with its controllers through an anonymised network on Internet addresses and servers and transit data.

A brief survey of the more damaging cyberattacks during the past decade-and-a-half with or without the Pegasus spyware can be revealing. Beginning with the 2007 devastating cyberattack on Estonia's critical infrastructure, this was followed by the Stuxnet worm attack a few years later on Iran's nuclear facility. The Shamoon virus attack on Saudi Aramco occurred in 2012. Thereafter, followed the 2016 cyberattack on Ukraine's State power grid; the 2017 Ransomware attack (NotPetya) which affected machines in as many as 64 countries; a Wannacry attack the same year on the United Kingdom's National Health Service; and the series of attacks this year on Ireland's Health Care System and in the United States such as 'SolarWinds', the cyber attack on Colonial Pipeline and JBS, etc.

Grave threat

With cyberweapons becoming the weapon of choice not only during a conflict but even during peacetime, matters have reached a tipping point. Cyberweapons carry untold capacity to distort systems and structures – civilian or military – and, most importantly, interfere with democratic processes, aggravate domestic divisions and, above all, unleash forces over which established institutions or even governments have little control. The Pegasus spyware is all this and more. For the present, it is hiding behind a cloak of anonymity, and the unwillingness of those to whom it has been sold to to acknowledge its misuse, but the reprieve is likely to be only temporary. Cyber methods which undermine capabilities can remain anonymous only for some, but not for all time. For the present, it may remain unrecognisable, but this will be only for a limited period.

Meanwhile, we must be prepared for, and guard against, a new epoch of cyber threats, employing newer, state-of-the-art cyberweapons, which will further intensify cyber insecurity across the board. As more and more devices are connected to networks, the cyber threat is only bound to intensify, both in the short and the medium term. What is especially terrifying is that instruments of everyday use can be infected or infiltrated without any direct involvement of the target. The possibilities for misuse are immense and involve far graver consequences to an individual, an establishment, or the nation. It is not difficult to envisage that from wholesale espionage, this would become something far more sinister such as sabotage.

Need for analysis

Dealing with the cyber threat, hence, deserves careful analysis and assessment. Plunging headlong into so-called solutions which have little rationale or depth is hardly the answer to critical threats posed by sophisticated spyware such as Pegasus. Dealing with 'zero day' vulnerabilities require far more thought and introspection than merely creating special firewalls or special phones that are 'detached' from the Internet. What is needed is a deeper understanding of not only cyber technologies, but also recognising the mindsets of those who employ spyware of the Pegasus variety, and those at the helm of companies such as the NSO. Short-term remedies are unlikely to achieve desired results.

With the advent of cyber weapons such as Pegasus, technology which is perceived as a friend could well become a matter of despair. At the pace at which cyber technology is evolving, erecting proper defences will prove difficult. Artificial Intelligence (AI) is often seen as a kind of panacea for many of the current problems and ills, but all advances in technology tend to be a double-edged sword. If truth be told, AI could in turn make all information warfare – including cyber related – almost impossible to detect, deflect or prevent, at least at the current stage of development of AI tools. Meanwhile, easy access to newer cyber espionage tools will add to the existing chaos. All this suggests that security in the era of ever-expanding cyberweapons could become an ever-receding horizon.

M.K. Narayanan, a former National Security Adviser and a former Governor of West Bengal, is currently Executive Chairman of CyQureX Pvt. Ltd., a U.K.-U.S.A. cyber security joint venture