The world is hardly wired for cyber resilience

A string of high-profile cyberattacks in recent months has exposed vulnerabilities in the critical infrastructure of even advanced nations. This has reinforced the need for improved defences against actual, and potential, cyberattacks by all countries across continents.

America under attack

1. Several high-profile cyber-attacks were reported from the United States during the past several months. Towards the end of 2020, for instance, a major cyberattack headlined 'SolarWinds' — and believed to have been sponsored from Russia — had rocked the U.S. It involved data breaches across several wings of the U.S. government, including defence, energy and state.
2. Before the U.S. could even recover from this breach, thousands of U.S. organisations were hacked in early 2021 in an unusually aggressive cyberattack, by a Chinese group Hafnium, which had exploited serious flaws in Microsoft's software, thus gaining remote control over affected systems.

Now, civilian targets

1. These attacks were all primarily on civilian targets, though each one was of critical importance. Obviously cyber, which is often referred to as the fifth domain/dimension of warfare, is now largely being employed against civilian targets, bringing the war into our homes.
2. Most nations have been concentrating to date mainly on erecting cyber defences to protect military and strategic targets, but this will now need to change.
3. The obsession of military cyber planners has been to erect defences against software vulnerabilities referred to as 'Zero-day', that had the capability to cripple a system and could lie undetected for a long time.
4. The most celebrated Zero-day software of this kind to date is Stuxnet, which almost crippled Iran's uranium enrichment programme some years back.
5. Today, other Zero-day software, no doubt exist, though little is known about them. What is, however, evident is that a whole new market currently exists for Zero-day software outside the military domain, and the world must prepare for this eventuality.

6. Defending civilian targets, and more so critical infrastructure, against cyberattacks such as ransomware and phishing, including spear phishing, apart from unknown Zero-day software, is almost certain to stretch the capability and resources of governments across the globe, somewhat in the manner that nations have been forced to find the resources and the methods to deal with the COVID-19 pandemic.
7. One related problem is that the distinction between military and civilian targets is increasingly getting erased and the consequences of this could be indeterminate.

Cyberwarfare against India:

1. Cyberwarfare is replete with several damaging methodologies. In the civilian domain, two key manifestations are ransomware and phishing, including spear phishing.
2. Ransomware attacks have skyrocketed, with demands and payments going into multi-millions of dollars. India figures prominently in this list, being one of the most affected.
3. Banking and financial services were most prone to ransomware attacks to date, but oil, electricity grids, and lately, health care, have begun to figure prominently.
4. Cybercriminals are becoming more sophisticated, and are now engaged in stealing sensitive data from targeted computers before launching a ransomware attack.

Need for data protection

1. Cybersecurity essentially hinges on data protection. As data becomes the world's most precious commodity, attacks on data and data systems are bound to intensify.
2. Building deep technology in cyber is essential. New technologies such as artificial intelligence, Machine learning and quantum computing, also present new opportunities.
3. Nations that are adequately prepared — conceptually and technologically — and have made rapid progress in artificial intelligence and quantum

computing and the like will have a clear advantage over states that lag behind in these fields.

4. Pressure also needs to be put on officials in the public domain, as also company boards, to carry out regular vulnerability assessments and create necessary awareness of the growing cyber threat.

Biden's Manichean vision

1. The G7 summit in Cornwall, U.K., was noteworthy for the cohesive vibe among member states, buttressed by their shared identity of being democracies.
2. In Mr Biden's Manichean vision, the world is at an "inflexion point between those who argue that autocracy is the best way forward and those who understand that democracy is essential".
3. Disproving the "false narrative" that dictatorships are faster and more efficient, and refuting autocrats who claim that the age of democracy is over, are the driving forces of Mr Biden's foreign policy.

An expanded coalition

1. To make sure that the messaging about team-building by democracies went across, the host of the Cornwall summit, British Prime Minister Boris Johnson, invited four other democracies as guest participants – Australia, India, South Korea and South Africa.
2. The combination of the G7 and the first three of these invitees has drawn attention to an expanded 'D10' coalition of democracies. USA promotes D10 as a necessary instrument to "bridge European and regional (Asian) approaches to Chinese challenges."
3. Since Japan is the only democracy from Asia within the G7, forging a D10 with Australia, India and South Korea could corral the U.S.'s European and Indo-Pacific allies to present a transcontinental counterweight to China.

Interdependent links

1. But what is different with today's 'new Cold War' is that power is more diffused around the world and economic interdependence transcends a neat division of the world into black (dictatorships) and white (democracies).
2. For example, despite being a U.S. ally and a democracy, South Korea is wary of joining a formal D10 or Quad-plus alliance because its economy is interwoven with that of China.
3. India, which has been wooing the Europeans to bring their economic and military heft to the Indo-Pacific, would be happy to see a combined trans-Atlantic and Indo-Pacific formation like D10 that could counterbalance Chinese hegemony.
4. But it cannot afford to alienate friendly undemocratic powers like Vietnam, Iran or Russia, all of which are vectors for India's ambitions of becoming a 'leading power' in the world.
5. And for that matter, the Americans and Europeans are themselves not undiluted upholders of democracy. The U.S.'s allies in West Asia remain notoriously authoritarian, and European countries still cultivate client dictatorships in Africa.

Politics is the art of the possible and so is geopolitics. The G7 and D10 are not idealistic alliances to spread democracy everywhere. They have to be selective in targeting adversaries and strike a balance among moral values, geo-strategic needs, and the complexities of the present multipolar world order.

Planning for a biosecure future

The growth of exponential technologies such as synthetic biology, artificial intelligence and nanotechnology is bound to change the theory and practice of national security. COVID-19 has quickened the inevitable.

Bioweapons:

1. Among the exponential technologies shaping the world today, the biological revolution is of exceptional importance. The rapid rise of synthetic biology in the last two decades and its still-to-be-understood implications haven't received sufficient attention from security studies or policy communities.

2. COVID-19 has further highlighted the biosecurity concerns of synthetic biology. The argument is not that COVID-19 originated in a lab, but that dangerous bio-weapons can come from labs.

Synthetic biology

1. That new organisms, biological parts and devices can be created or that existing natural life forms can be redesigned should ideally be the subject matter for scientists to concern themselves with or for ethicists to debate.
2. But today, there is a growing realisation that exponential technologies have hitherto unforeseen national and global security implications. In 2014, for instance, the U.S. Department of Defense categorised synthetic biology as one of the six 'disruptive basic research areas' even though linkage between national security and synthetic biology is yet to become an agenda item in mainstream national security debates.
3. There is a need to carefully review, especially in the wake of the pandemic, the biosecurity systems in place where such technologies are in use.
4. Accidental leaks of experimental pathogens are another concern. Insufficiently trained staff, inadequately safeguarded facilities, and lack of proper protocols could all be behind such leaks.
5. The reality is that there has been very little focus on threats emanating from biological sources. Contrast this with the focus on nuclear weapons, facilities and material. Not only are they tightly controlled but are also the subject of strong global regimes.
6. This is despite the fact that a well-orchestrated biological attack could have serious implications even though it would be less 'spectacular' since its effects are less immediate. This was before synthetic biology came into play. A well-planned attack using highly infectious pathogens synthetically engineered in a lab could be disastrous.

Difficult questions:

1. How easy would it be to pin responsibility on a specific actor if the incubation period is high and the pathogen can be modified to hide its origin?
2. Unlike the nuclear domain, the fields of biology or synthetic biology are not regulated internationally despite growing military interest in synthetic biology applications and their potential misuse.

3. The 'weapon of mass destruction (WMD) capability of bio-weapons has been long recognised but very little has been done by the international community about it.
4. Of the three types of WMD, nuclear weapons have received the maximum safety and security attention given the treaty and institutional arrangements associated with it.
5. Chemical weapons come next. There is an international convention and an implementing body. However, when it comes to bio-weapons, all we have is the Biological and Toxin Weapons Convention (BTWC) of 1972 with no implementing body.
6. The BTWC does not have a verification clause, nor does it have clearly laid down rules and procedures to guide research in this field.
7. In BTWC, while bio-weapons are banned, research for medical and bio-defence purposes are allowed. While this is understandable, the problem is that there is a thin line between bio-defence research and bio-weapons research.
8. Since bio-defence research routinely uses pathogens and toxins for experimental purposes, processes, know-how and outcomes of bio-defence research could potentially be used to create bio-weapons, especially with the new advancements in synthetic biology.
9. More so as the pharmaceutical industry has vehemently opposed any intrusive inspection regime.

India uniquely unprepared

1. India is in a uniquely disadvantaged position compared to the more developed countries in this area given poor disease surveillance, insufficient coordination among various government departments dealing with biosecurity issues, and the pathetic state of the healthcare system.
2. India has multiple institutions dealing with biosafety and biosecurity threats but there is no coordination among them.
3. For instance, the implementation of biosafety guidelines is the responsibility of the Science and Technology Ministry and the Environment Ministry. However, labs dealing with biological research are set up under the Indian

Council of Medical Research and the Indian Council of Agricultural Research, which are under the Ministries of Health and Agriculture, respectively.

4. This highlights two issues pertaining directly to biosecurity. One, the multiplicity of bodies and ministers makes coordination difficult, especially in the absence of an empowered coordinating body.
5. Two, given the rising risk of diseases of zoonotic origin, the traditional ministry-wise separation might not be useful. Another important question is whether India, with its porous borders and ill-trained border control institutions, is prepared for defending against pathogens or dangerous biological organisms or agents arriving from abroad. COVID-19 should serve as a wake-up call.