The world is witnessing two simultaneous revolutions – the explosion of information in the public domain and the destructive power of information. The possibilities of mind control and impossibilities of suppressing information are going hand-in-hand as Wikileaks and the events in the Arab world illustrate. The nation-State can no longer prevent information from burgeoning. The technicalities of a computerised world are eagerly sought by young minds, unfortunately not always with altruistic intentions as hacking shows. It is an extremely useful tool in the growth and development of the human race which the sum of its contradictions cannot obliterate.

Four centuries ago, the English statesman-philosopher Francis Bacon had pertinently claimed that – "Knowledge is power". At the start of the 21st century, it is proving correct both in the context of the acquisition and dissemination of knowledge across the world. The world has been confronted with a number of technological developments in the last two decades especially in the field of computers, communications and software. In turn, this has impacted the cost of processing and transmitting information. The key characteristic of the information revolution is not the speed of communications but the enormous reduction in the cost of transmitting information which has become negligible. Hence the amount of information that can be transmitted worldwide has become effectively infinite.

Hackers and political activism

In 1999, 1,500 groups and individuals planned a significant part of their campaign on the Internet and disrupted an important meeting of the World Trade Organisation in Seattle. In 2000, a young hacker in the Philippines launched a virus that spread around the world causing US$ 4 billion to US$ 15 billion in damage in the United States alone. In 2010, Twitter, Facebook and YouTube orchestrated a people's movement in Tunisia and Egypt resulting in the overthrow of years of authoritarian rule. In India, the expose of the 2G spectrum scam resulting in the arrest of A. Raja, then Information and Telecommunication Minister; the annulling of the controversial S-Band spectrum deal between the Indian Space Research Organisation and Devas Multimedia; the resignation of the Chief Vigilance Officer, P. Thomas, after it was revealed he was charge-sheeted in a multi-crore palmolein oil scam have all occurred over the last six months. In all these instances, the Indian government has been forced into action in the wake of immense public scrutiny. In April 2011, Indian social activist Anna Hazare, launched the latest crusade against corruption, a lonely battle he was fighting since 1969. Again, the State was forced to accede to the demands of creating a committee for discussing the Bill on setting up a Jan Lokpal, an independent body with power to investigate and punish corruption. Interestingly, the significant reason for the State to respond favourably in this instance was the immense support of the people, especially the youth, from all corners of the country for Anna Hazare.

There has been growing competition among major powers to achieve both information assurance and information dominance. The State has always controlled information relating to every sphere of development. Hence, traditionally, information has been restricted to the elite within the State. The public has been largely kept out of the decision making. Additionally, there was a lack of communication structure and access to technologies of information and communication which hindered society from taking a keen interest in public affairs.

Dr. Venkateshwaran Lokanathan

INFORMATION DOMINANCE: POWER OF THE FUTURE?

Freedom of information

The dramatic shift in the linked technologies of computing and communications has now posed a new challenge to the existing nature of governments and sovereignty. In the current scenario, it will become extremely difficult for the State to withhold information for a long time. Economies and information networks have changed more rapidly than governments, with their scale growing much faster than that of sovereignty and authority. It has, simultaneously, thrown open new challenges for maintaining secrecy particularly on issues related to national security. To put it succinctly, world politics has been transformed by the advent of new technology and State policies are now required to accommodate and adjust its interests accordingly.

Globalisation

It is remarkable that the rapid technological developments have been ideally complimented by the emergence of a globalised world. Globalisation in the 21st century has distinct characteristics. Thomas Friedman described it as "farther, faster, cheaper and deeper". India opened its market and liberalised its economic policies in 1991. This has resulted in the growth of worldwide networks of economic interdependence involving people from more regions and social classes. It is obvious that direct public participation in both domestic and global affairs has increased. There is a vast expansion of transnational channels of contact at multicontinental distances, generated by the media and a profusion of non-governmental organisations. The concept of contemporary globalisation has been provided lots of semblance in the on-going information revolution. As the Indian State begins to shape its foreign policy for the 21st century it will have to respond to issues that involve greater complexity, more

In India, efforts in the direction of a national cyber security strategy are not visible this far. The government has set up CERT-In as a division of the Ministry of Information Technology which is being nurtured as the nodal security agency. However, there is an urgent need to develop cooperation between different security organisations in such a manner that the national Cyber Space remains secured. If such a collaborative structure is to be built up then there is also the issue of whether it is feasible for the government sector to join hands with the private sector. Effective Public-Private sector cooperation is therefore one of the key challenges in building the national cyber security infrastructure

uncertainty, shorter response times and broader participation by groups and individuals.

Non-State actors

Another interesting offshoot has been the globalisation of existing problems characterised by inequitable development between the north and the south and the rich–poor divide existing even within countries. The recent surge in protests is, in part, also a reaction to the changes produced by economic integration. Historian Karl Polanyi argued strongly in his study "The Great Transformation" that the market forces unleashed by the industrial revolution and globalisation in the nineteenth century has produced not only great economic gains but also great social disruptions and political reactions. Unfortunately many such reactions have taken a violent form after years of suppressed frustrations. The State, in many instances, has also added fuel to fire by making forceful attempts at crushing such protests which has only fuelled further violence. The violent nature of the Naxal movement in states of central India, the United Liberation front of Assam (ULFA) and the Nagas in Nagaland until recently, characterised by years of neglect towards the larger north-east region, are significant representations. Simultaneously, the presence of global terror networks established by organisations such as the Al Qaeda, Lashkar-e-Toiba, Jaish-e-Mohammad, al–Ummah, Hezbollah, Muslim Brotherhood, Harkat–ul-Mujahideen has also created a rapidly deteriorating security environment. Ironically, these organisations have also begun to effectively use ICT and the new media to propagate their ideology which in turn has assisted in the process of indoctrination and increasing their membership. Thus, in this contemporary environment, the State faces a critical question. How to protect important information that endangers national security from non-State actors?

New challenges

The emergence of the concept of Cyber Space in contemporary world politics has created a difficult environment where many nations have been confronting challenges emanating from e-governance and e-commerce from the perspective of their national security.

First, a range of individuals and entities, from hackers to large corporations, have the ability to develop the code and norms of the Internet partly outside the control of formal political institutions today. The development of transnational corporate intranets behind firewalls and encryption represents private appropriations of a public space. They have simply added a layer of relations that sovereign States are finding challenging to effectively control. Today, the Internet rests on servers located in specific nations and various government laws affect access providers. The current wrangling between the Indian government and the Canadian owners of the BlackBerry services, Research In Motion, over security concerns is a case in point. Hence, in the age of the Internet, the changing role of political institutions is likely to be a gradual process.

Second, there seems to be a worrying trend that has emerged because of the lack of well trained professionals or experts. Deployed technology illustrates a lack of understanding on how to build systems that can be trusted to work correctly despite adversarial action. Nevertheless, more important processes are being rushed into computing systems. The increase in computing systems' performance and online storage further complicates matters by providing more systems to protect and greater temptation for those who could abuse those systems.

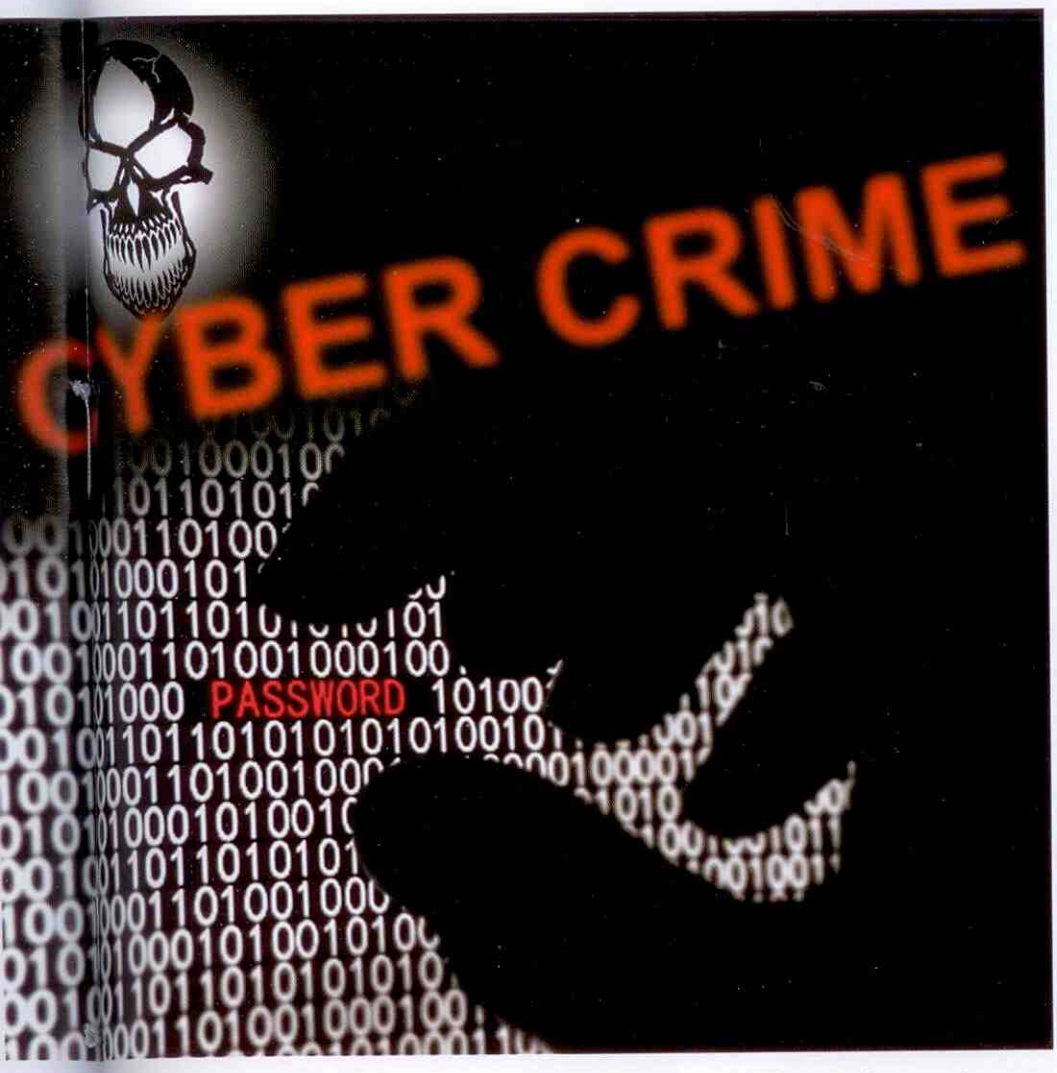
Third, computing is also plagued by the challenges of epidemic-style attacks. Spam makes it hard to read email while denial-of-service (DOS) attacks often brings down critical sites at inopportune times. Viruses and worms continue to plague systems and critical infrastructure (such as ATMs and emergency response systems) that previously had resisted them.

Fourth, the challenge is also asymmetric - attackers can be local and they require few resources and entry points, whereas defenders must be global and organised. Hence, as sensitive operations are moved onto networked general-purpose machines, on what grounds can stakeholders trust that the networks can resist dedicated attackers?

Risk management

Fifth, the lack of well-founded techniques to evaluate whether enough is spent on security technology, or what the current level of risk is as compared to earlier. Hence, there is an urgent requirement to create a quantitative information systems risk management. This would enable government, industry and consumers to make rational decisions about security investment.

Sixth, technology is becoming increasingly complex today. Even an experienced user is having trouble conceptualising exactly what services the machine offers right now on the



network and what pull-down menus and configuration files to change to steer those services into a more acceptable state. This situation will only get worse as we continue to extend the analysis to less savvy users in rural India. Human users will be unable to make rational choices if they cannot understand the systems.

Seventh, there should be freedom to choose actions that help manage privacy. Moving activity into a networked computing environment, with machines and software representing many stakeholders makes it much harder to delineate exactly what's involved in these actions. Where does private information go today? Does one know it was going there? Social values need to dictate our technology and not the other way around.

Cyber crimes

Eighth, there is a lack of awareness among law enforcement agencies about the seriousness and deadly intent of cyber-crimes. Additionally, in the few cases where Cyber Crime cases have been initiated, lack of coordination among these agencies has often hindered speedy investigations. When Cyber Crimes are committed with mobile network, it is often difficult to convince the mobile service providers that they are responsible for assisting the Police in the investigation. Many of them do not even recognise mobile crimes as Cyber Crimes and therefore fail to appreciate their legal obligations. In the private sector, whenever crimes are reported, companies, concerned about their own reputation than public good, do not register a complaint nor enable a proper investigation. Bankers hide any frauds that occur in their network for the fear of losing public confidence. The software developers also contribute in their own measure to the insecurity in the Cyber space by supplying software that has many security weaknesses.

Effective counter-measures

In India, efforts in the direction of a national cyber security strategy are not visible thus far. The government has set up CERT-In as a division of the Ministry of Information Technology which is being nurtured as the nodal security agency. However, there is an urgent need to develop cooperation between different security organisations in such a manner that the national Cyber Space remains secured. If such a collaborative structure is to be built up then there is also the issue of whether it is feasible for the government sector to join hands with the private sector. Effective Public-Private sector cooperation is therefore one of the key challenges in building the national cyber security infrastructure. There is another lurking danger where our critical IT infrastructures such as the missile launching stations, the defense support IT systems could be under threat of an Electronic warfare. It is already speculated that China is training intensely towards unleashing such a war in the foreseeable future.

Crucially, there is a need for central agency that will supervise and coordinate the activities of the sub-divisions at the State level. This will include highest priority infrastructure divisions like the security requirements of the armed forces, select installations of national importance such as the nuclear power stations, rocket launching stations, AIR and Doordarshan. All other assets of the government such as e-governance support will come under lower priority infrastructure. There is also an urgent need to educate and create a specialised arm of the police that coordinates and handles investigations into cyber-crimes both at the central and state level. Two independent supervising bodies also need to be established to overlook cyber security in the private sector and even at an individual level. DSA

The writer is currently Senior Lecturer in the Department of Geopolitics and International Relations at Manipal University, Manipal, India. He has also worked as a Research Officer at the Institute of Peace and Conflict Studies, New Delhi. His areas of interest include broader contours of International Security Affairs with specific focus on the United States, China and South Asia.