**Pakistan’s looming cyber threat**

[Mohsin Durrani](https://dailytimes.com.pk/writer/mohsin-durrani/" \o "More Articles by Mohsin Durrani)

OCTOBER 5, 2019

Pakistan’s digital infrastructure is vulnerable. About cyber espionage, one knows who, how, where, and why it matters? But there is paucity of knowledge about “what to do”? Pakistan does have cyber-crime laws but unfortunately it is not being implemented effectively, rather it is not evolving at the same pace that is required to keep up with the changing times.

In the 21st century, nations, nonstate actors, and individuals have a new avenue to engage in conflict. The development of the Internet has had many unforeseen effects on human society, enabling massive changes in communications, commerce, and conflict. So far, the Internet has not fundamentally changed human nature; it has only allowed for a new means of engaging in normal human behaviour, including some of the worst human activities. Thus, it is unsurprising that humans have chosen to continue their criminal, espionage, sabotage, and warfare activities in the new cyber domain.

As more devices are connected and societies become more dependent upon cyber networks, the possibilities for causing harm grow in proportion. Further, because the Internet is by definition an international network that does not halt at national borders, it blurs the line between domestic and global activities, pushing past the assumed limitations of domestic and international law. Because a nation may choose to respond to a cyber-attack by retaliating in the physical domain, cyber warfare offers a certain potential for crossover effects. Ultimately, whether an attack is perceived as an irritant or an act of war will largely depend on the preferences, motivations, and capabilities of the victim more than the intentions of the actor.

The cyber domain has special characteristics that make it a unique arena for human conflict. Unlike the physical domains (land, sea, air, and space), the cyber domain is entirely artificial and it remains an evolving platform. Although certain behaviours in cyber space are governed by the limits of what can be performed within a computer network, it is unclear whether other forms of government truly apply to the Internet. Certainly, the establishment of computer networks has challenged many assumptions regarding the limits of legal and ethical behaviour. Because the Internet has outgrown all projections for both its utility and its dangers, it is impossible to predict how it will develop in even the near future, much less over the remainder of the 21st century.

Because the cyber domain is entirely manmade, it is not governed by the same properties as the physical world. In fact, there are no rules within the cyber domain that cannot be changed, either by altering the hardware that creates the environment or changing the programming that controls it. Given this changing nature of the cyber environment, developing a national cyber strategy to secure a country from cyber-attacks is a continual problem. The only sure way to become immune to cyber-attack is to sever all connections to the cyber domain but such a drastic decision would also essentially remove a nation from the modern world. Thus, nations are forced to engage in the cyber domain, regardless of preferences, priorities, or national capabilities.

*With hyperactive social media in Pakistan, it is critical to study the potential and limitations of the internet. It is crucial that academics try and better understand the landscape of internet in Pakistan*

Cyber assets are typically associated with communications, economic activities, and maintaining vast amounts of information, and cyber-attacks are thus most commonly assumed to be new forms of espionage or crime. However, cyber networks are increasingly able to influence the physical world through the control of infrastructure assets such as electrical grids, meaning that a cyber-attack can potentially inflict harm on not only computer hardware but also the people living in the cyber-enhanced environment. Whereas earlier cyber-attacks might be considered a problem best addressed by intelligence agencies or law enforcement, these more advanced cyber-attacks might cross the threshold into warfare, particularly if they directly or indirectly cause the loss of human life. Already, cyber-attacks are being used as an enhancement mechanism to enable or improve kinetic attacks in the physical world, but soon, they may be utilized in place of conventional violence, achieving the same ends without incurring the same risks to the attacker.

In the cyber domain, it is difficult to distinguish between the uniformed representatives of a nation and other participants acting on their own motives. As such, there is at the very least a gap in the Law of Armed Conflict (LOAC) that requires modifications if they are to cover the entire range of potential cyber conflicts. Cyber-attacks might not discern between legitimate warfare targets, such as government and military entities, and illegitimate targets, such as civilians not directly related to the war effort, due to the uncontrolled nature of some cyber-attacks. As technology advanced and critical military, government, and economic systems became more reliant on technology, the need for increased security became an important factor of national security.

Although many countries all over the world are committing cyber espionage, the United States, Russia, and China are considered the most advanced and most prolific cyber spies. Growth and proliferation of such technologies present a serious threat to world peace. There is an urgent need for nations of the world to come together to agree on reasonable restrictions to prevent disasters.

The cyber domain is largely a positive innovation, for most of its users, the Internet is a vast, poorly understood environment. Most computer owners do not realize the inherent dangers that it represents or how their interaction with sites on the Internet might enhance the ability of malevolent actors to carry out acts of crime, espionage, sabotage, terrorism, and warfare. While this should not scare citizens into departing the cyber domain entirely, in some ways, the subjects discussed in this work should remind users that there are often far greater consequences to seemingly innocent activities in the cyber domain.

They should be aware of the types of organizations using the Internet for their own purposes, ranging from hostile nation-states seeking avenues of attack and new means of information theft to terrorist organizations attempting to recruit new members and spread their propaganda. Cyber criminals, too, have found the Internet to be a vast new trove of potential targets, many of whom unknowingly volunteer their information without regard for the dangers involved.

In Pakistan There is also a lack of awareness about the law. There is need of holding workshops and seminars to create awareness among the masses. There must be severe actions against criminals. Vulnerability assessment of famous Apps for smart phone may be done. “National cyber security awareness day” be organised to make people aware of what this cyber age is all about. Online dangers to children include exposure to illegal or inappropriate material, stranger danger, identity theft, invasion of privacy, harassment and cyberbullying.

Awareness about cyber security need to start from the school levels to better equip children from an early age. Improving and changing current information-security behaviours requires more than providing teachers with information to teach. Teachers must be able to understand and apply the advice, and they must be motivated and willing to do so. If we’re really serious about cybersecurity education in schools, it needs to become part of the school curriculum, and teachers need to be supported in a meaningful way to teach it.

With hyperactive social media in Pakistan, it is critical to study the potential and limitations of the internet. It is crucial that academics try and better understand the landscape of internet in Pakistan. Cyber-attacks and defence should eventually be part of Pakistan’s National Security structure. The Civilian and Military setup in collaboration with the Private Sector need to devise a robust and an ever-evolving cyber threat management mechanism that can aide in countering threats both local and international in nature.

*The writer is an Independent analyst. With interests in Regional and International Affairs*