Need for Implementing Control on Political Parties Funding

Kaukab Jamal Zuberi
Chief Editor

Internet has become a part of our life. We use internet to search information, deliver education, communicate with each other, doing medical operations, entertainment and monitor various devices ranging from CCTV cameras to pacemakers. Cyber world therefore, is a space on which we are depending by one way or other every single day. Among the broadband networks, beneath us, and the wireless signals around us, the local networks in our schools, hospitals and businesses, and the massive grids that power our nation, classified military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than any time in human history. It is a great irony of our cyber age that the technology which enables us to create, build and facilitate our lives also empowers those who would disturb and destroy.

So, cyberspace is real. And so are the risks that come with it.

Cyber space has been declared as the fifth domain of war. Any attack on the cyber space is now considered as the attack on the sovereignty of the country. Next wars will also include cyber-attack directed towards the critical infrastructure of the enemies.

Critical infrastructure as defined in Prevention of Electronic Crime Act 2016 is defined as follows:

""Critical Infrastructure" means critical elements of infrastructure namely assets, facilities, systems, networks or processes, loss or compromise of which could result in,:-

(a) Major detrimental impact on the availability, integrity or delivery of essential services, including those services, whose integrity, if compromised, could result in significant loss of life or casualties, taking into account significant economic or social impacts; or

(b) significant impact on national security, national defense, or the functioning of the state".

Destruction of critical infrastructure may result in provision of critical services to the citizens and/or result in huge economic losses to the country. It may also cause huge losses of life.

Types of Cyber Warfare:

Cyber Espionage

Traditional espionage is not an act of war, nor is cyber-espionage, and both are generally assumed to be ongoing between major powers. Despite this assumption,

some incidents can cause serious tensions between nations, and are often described as "attacks". For example

i. Massive spying by the US on many countries, revealed by Edward Snowden.

ii. After the NSA's spying on Germany's Chancellor Angela Merkel was revealed, the Chancellor compared the NSA with the Stasi.

iii. The NSA recording nearly every cell phone conversation in the Bahamas, without the Bahamian government's permission, and similar programs in Kenya, the Philippines, Mexico and Afghanistan.

iv. The security firm Area 1 published details of a breach that compromised one of the European Union's diplomatic communication channels for three years.

Out of all cyber-attacks, 25% of them are espionage based

Sabotage

Computers and satellites that coordinate other activities are vulnerable components of a system and could lead to the disruption of equipment. Compromise of military systems, such as C4ISTAR components that are responsible for orders and communications could lead to their interception or malicious replacement. Power, water, fuel, communications, and transportation infrastructure all may be vulnerable to disruption. According to Clarke, the civilian realm is also at risk, noting that the security breaches have already gone beyond stolen credit card numbers, and that potential targets can also include the electric power grid, trains, or the stock market.

In mid-July 2010, security experts discovered a malicious software program called Stuxnet that had infiltrated factory computers and had spread to plants around the world. It is considered "the first attack on critical industrial infrastructure that sits at the foundation of modern economies," notes The New York Times.

Denial-of-Service attack

In computing, a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. DoS attacks often leverage internet-connected devices with vulnerable security measures to carry out these large-scale attacks. DoS attacks may not be limited to computer-based methods, as strategic physical attacks against infrastructure can be just as devastating. For

example, cutting undersea communication cables may severely cripple some regions and countries with regards to their information warfare ability

Electric Power Grid

The electric power grid is susceptible to cyberwarfare. The United States Department of Homeland Security works with industries to identify vulnerabilities and to help industries enhance the security of control system networks. The federal government is also working to ensure that security is built in as the next generation of "smart grid" networks are developed.

Propaganda

Cyber propaganda is an effort to control information in whatever form it takes, and influence public opinion. It is a form of psychological warfare, except it uses social media, fake news websites and other digital means. In 2018, Sir Nicholas Carter, Chief of the General Staff of the British Army stated that this kind of attack from actors such as Russia "is a form of system warfare that seeks to de-legitimize the political and social system on which our military strength is based".

Jowell and O'Donnell (2006) state that "propaganda is the deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behavior to achieve a response that furthers the desired intent of the propagandist". The internet is the most important means of communication today. People can convey their messages quickly across to a huge audience, and this can open a window for evil. Terrorist organizations can exploit this and may use this medium to brainwash people. It has been suggested that restricted media coverage of terrorist attacks would in turn decrease the number of terrorist attacks that occur afterwards.

Economic Disruption

In 2017, the WannaCry and Petya cyber-attacks, masquerading as ransomware, caused large-scale disruptions in Ukraine as well as to the U.K.'s National Health Service, pharmaceutical giant Merck, Maersk shipping company and other organizations around the world. These attacks are also categorized as cybercrimes, specifically financial crime because they negatively affect a company or group.

There is a controversy against the term “cyber warfare”. Some believe it is not the right term. Eugene Kaspersky, founder of Kaspersky Labs, concludes that "cyberterrorism" is a more accurate term than "cyberwar". He states that "with today's attacks, you are clueless about who did it or when they will strike again. It's not cyber-war, but cyberterrorism.

In either way, it is the responsibility of the government to develop an effective cyber security strategy and develop a qualified manpower in various domains of cyber security.

A recent study conducted by Comparitech

has revealed that Pakistan ranks 7th among the countries having the worst cybersecurity. This makes Pakistan one of the most unprotected countries. Recent attack on FBR was one of the many attacks successfully conducted on Pakistani critical infrastructure. The cyber-attacks can result in very high losses. If we do not develop a comprehensive cyber security policy and give incentives to develop high level of professionals in this team, we keep on risking to compromise our cyber space. Pakistan is at risk and we need to act fast.