Name of Country: the Islamic Republic of Afghanistan

Committe: GA:1 DISEC

Agenda item: Weaponization of Data and Cyber Security

Cybersecurity began in the 1970s when researcher Bob Thomas created a computer programme called Creeper that could move across ARPANET’s network, leaving a breadcrumb trail wherever it went. Ray Tomlinson, the inventor of email, wrote the programme Reaper, which chased and deleted Creeper. Reaper was the very first example of antivirus software and the first self-replicating programme, making it the first-ever computer worm. With the internet becoming available to the public, more people began putting their personal information online. Organised crime entities saw this as a potential source of revenue and started to steal data from people and governments via the web. By the middle of the 1990s, network security threats had increased exponentially and firewalls and antivirus programmes had to be produced on a mass basis to protect the public.In the early 2000s crime organisations started to heavily fund professional cyberattacks and governments began to clamp down on the criminality of hacking, giving much more serious sentences to those culpable. Information security continued to advance as the internet grew as well but, unfortunately, so did viruses. The cybersecurity industry is continuing to grow at the speed of light. The global cybersecurity market size is forecast to grow to $345.4bn by 2026 according to Statista. Ransomware is one of the most common threats to any organisation's data security and is forecast to continue to increase

In 2009, MCIT established the first Cyber Emergency Response Team (CERT) in Afghanistan and it was officially named as AFCERT. The mandate of AFCERT was to fight against cyber threats and crimes and provide awareness and solutions on cyber security to the government and private sector. In its first two years of operation, AFCERT submitted an official report to the MCIT senior management regarding an upsurge in the cyber and electronic crimes in the country. In order to fight the said crimes, it was vital to conduct a risk assessment of all government ICT infrastructures and come up with a solution to mitigate those risks. AFCERT’s proposal on preparing a draft of Cyber Security Strategy for the country was accepted by the MCIT and ICT Council and to this end the MCIT and ICT Council established a committee. Our mission is that to protect and assure data, information and IT infrastructure security in Afghanistan’s cyberspace, enhance capacities to prevent and response to cyber threats, protect the children and youth of Afghanistan in cyberspace, mitigate the risk of vulnerability, damage from cyber threats and incidents through a variety of standardized institutional structures, policies, procedures, people, technologies and administrative process. There are a total of 5 action items scheduled to take place between 2014-2015. The deadline for some of the actions are determined and those actions which are envisioned to be repeated periodically and/or are of chronic

occurrence are highlighted in particula

Cyber security solutions are technological tools and services that help protect organizations against cyber attacks, which can result in application downtime, theft of sensitive data, damage to reputation, compliance fines, and other adverse consequences. As Sun Tzu said “ The art of war teaches us to rely not on the likelihood of the enemy’s not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.” In order to protect our world on cyber security, not only a few countries, but all countries within the UN should participate. That is why we have attended the meeting of such a committee.