HEADLINE CATEGORY	SUB-CATEGORY	SUB-SUB-CATEGORY
National Cyber-Security Strategies	• National cyber programmes	• Guides on writing a national strategy
		• Cyber capability assessment tools
		• Example national strategies
	• public/private partnerships,	
	• public awareness campaigns,	
	• national skills development	
Cyber crime	• Development of law enforcement agency skills and capacity	
	• Detection and reporting of cybercrime	• Public awareness campaigns
		• Information sharing and public/private partnerships
	• Forensics and digital evidence	• Forensic Tools & Training
		• Obtaining and handling digital evidence
	• Prosecution of cybercrimes	• Training of prosecutors
		• legal jurisdiction in a digital world.
		• digitally enabled crime
		• Admissibility of digital evidence in court
		• Offender management and rehabilitation of hackers
	• Legal frameworks & statutory powers of investigation	• Illegal access; Illegal interception; data interference; system interference; misuse of devices; computer-related forgery/counterfeiting; computer-related fraud; child sexual abuse; offences related to infringements of copyrights and related rights;

		• statutory powers of investigation and evidence collection for; expedited preservation of stored computer data; expedited preservation and partial disclosure of traffic data; production order; search and seizure of stored computer data; Real time collection of traffic data; interception of content data
	• Child online protection	
	• International and public/private collaboration	• Legislation supporting international cooperation; mutual legal assistance
		• **International collaboration on threats**
		• Botnets
		• Spam
		• Fraud
		• Hacktivism
Security & Resilience	• Critical Information Infrastructure Protection	• CIIP policy and guidance
		• Supply chain verification and policy
		• Legislation, regulation
		• Information sharing and collaboration; Warning and Reporting Points
		• exercises
	• Computer Emergency Response Teams	• Guides to establishing CERTs
		• Exercises and development of CERTS

		REACTIVE SERVICES
		• Alerts & warnings
		• Analysis, response and coordination for:
		  - Incident Handling
		  - Vulnerability Handling
		  -Artifact Handling

		PROACTIVE SERVICES • Announcements • Technology watch • Security audits or assessments • Configuration and maintenance of security tools, applications &

		infrastructure
		• Development of security tools
		• Intrusion detection Services
		• Security related information dissemination
		Security Quality Management Services
		• Risk analysis
		• Business continuity and disaster recovery planning
		• Security consulting
		• Awareness building
		• Education/training
		• Product evaluation/certification
	• Information Assurance and network defence	• Policy, governance, procurement & standards
		• Infrastructure & hardware assurance
		• Testing
		• Patching & monitoring
		• Authentication & trust mechanisms
International Security	• Military operations/ defence	
	• Counter espionage	
	• Cyber terrorism	
	• Confidence Building Measures	
	• Norms of behaviour and application of law in cyberspace	
Governance, Economic Growth & Social Benefits	• National and international internet governance	• Principles & guidelines for internet governance
		• Governance fora
	• Social benefits	• Online freedom, privacy and data protection aspects of cyber-security
	• Economic Growth	• Protection of intellectual property
		• Drivers of online economic growth