this involves **the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks**. It aims to reduce the risk of cyber attacks and protect against the unauthorised exploitation of systems, networks and technologies. .

This strategy explores the idea of having a strong and robust cyber-ecosystem where the cyber-devices can work with each other in the future to prevent cyber-attacks, reduce their effectiveness, or find solutions to recover from a cyber-attack.

Such a cyber-ecosystem would have the ability built into its cyber devices to permit secured ways of action to be organized within and among groups of devices. This cyber-ecosystem can be supervised by present monitoring techniques where software products are used to detect and report security weaknesses.

**symbiotic structures of secure cyber-ecosystem**

**● Automation**

**● Interoperability**

**● Authentication**

* **Automation** − It eases the implementation of advanced security measures, enhances the swiftness, and optimizes the decision-making processes.
* **Interoperability** − It toughens the collaborative actions, improves awareness, and accelerates the learning procedure. There are three types of interoperability −

●Semantic (i.e., shared

lexicon based on common understanding)

* Technical
* Policy − Important in assimilating different contributors into an

inclusive cyber-defense structure.

* **Authentication** − It improves the identification and verification technologies that work in order to provide −
* Security
* Affordability
* Ease of use and administration
* Scalability
* Interoperability