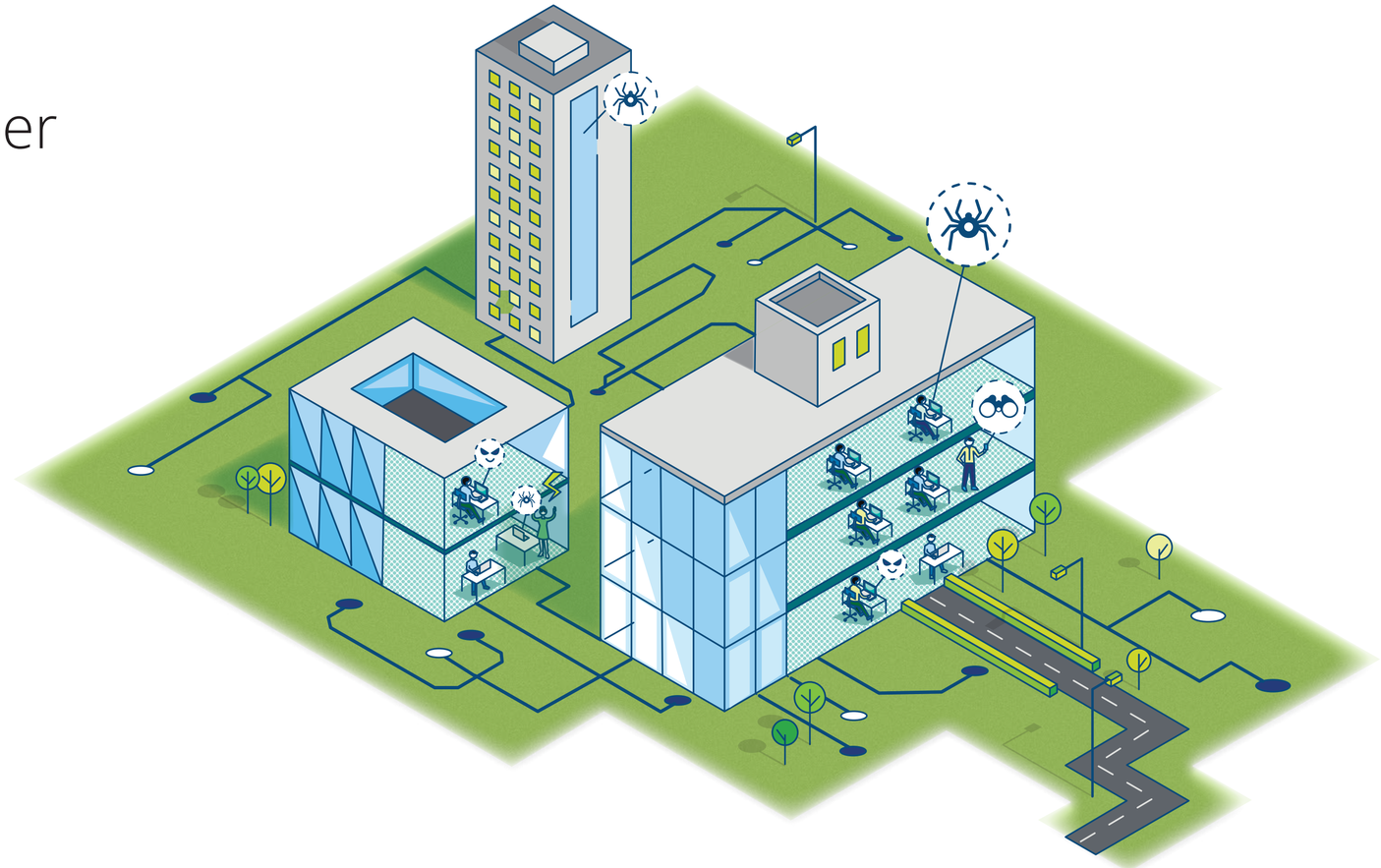
Cyber 101

Develop a view on Cyber

1982	**CIA alters software to cause explosion**
1998	**First Internet Worm: The Morris Worm left computers defective**
2008	**Pentagon discovered data breach of US military computers in Middle East**
2010	**First military cyber weapon, Stuxnet to control and destroy machinery**
2012	**Red October -Worldwide malware collected info with Microsoft tools**
2013	**The New York Times' systems were hacked and staffs' passwords acquired**
2014	**Cyber espionage used by Russia to disable Ukraine's communications**
2016	**More than 1 billion email accounts on Yahoo compromised with users' information breached**
2017	**Wannacry Ransomware**



Hunting in the Cyberspace

One of the largest cyberattacks, WannaCry Ransomware, signifies a wake-up call to all organisations alike, requiring both global responsibility and attention to prevent future episodes. We hope to shed light on the fundamentals of cyber security with this 8 part Edu-series to help you understand and protect your data.

Cyberattacks, unlike physical warfare, transcends national borders by compromising computer systems and networks. In this interconnected digital sphere, they threaten the very infrastructures that nations and corporations depend on. Data theft, manipulation of networks and disabling online platforms have amounted to considerable repercussions.

You can find some noteworthy events on the left.

Undeniably, major cyber infringements also demonstrate the vulnerability of national systems. The growing trend of political cyberattacks has formed a new field of spying: cyber espionage – superpowers have engaged cyber software such as Stuxnet, Flame and DuQu, in an attempt to monitor, collect and control its target. Cyber espionage has been around for some time now but the acts of disruption have been growing into international cyber wars that might be spinning out of control.