Tech domain	Characteristics & features	Information risks	Security controls
Information (**IT**)	● Conventional business & personal IT systems processing commercial & personal information ● Desktop & portable PCs, servers, LANs & WANs (almost exclusively using the global Internet) ● Networks are designed to facilitate the communication & sharing of data & information services ● Regularly updated ● Short lifecycles with frequent hardware & software updates	● Data confidentiality, integrity & availability concerns, with security implications for systems, network, applications, usage, management, maintenance *etc*. ● Long history of social engineering, malware, hacking, bugs & flaws *etc*. ● Long history of coercion, both protection rackets (costly security technology & service options) & malicious exploitation ● Tricky to secure information effectively without unduly restricting availability & hence legitimate exploitation ● Attacks often $-motivated: phishing, ransomware, fraud & insider threats ● Most incidents accidental or incidental ● Impacts can include direct & indirect losses, lost productivity, incident management & recovery costs, forensics, reputation/brand damage	● Long history of controls to protect sensitive and/or valuable data against all manner of harmful incidents involving loss of confidentiality, integrity, availability, control ● Ensure network & business system uptime ● Administer security *e.g.* access rights, monitoring ● Comply with applicable laws & regulations ● Conform with applicable contracts, agreements & policies, ethical codes ● Patch management - routinely applying security patches across the dispersed business (creating widespread problems if patches fail) ● Real-time system & network monitoring tools to detect anomalous behaviour & identify potential threats ● Established incident response plans for data breaches or system outages

Tech domain	Characteristics & features	Information risks	Security controls
Operational (OT)	● Computer systems/devices that interact with the physical world, monitoring or controlling actuators, valves, switches, motors *etc.* such as industrial control systems (SCADA/ICS), robotics, building management systems, HVAC, fire & access control mechanisms ● Primary concern is human safety, followed by operations, production or service continuity ● Often required to run 24x365 for safety, security & productivity reasons ● Often encapsulated or enclosed for harsh environments, some being embedded within machinery or physically remote, & hence difficult to access physically ● Lifecycles can extend to decades, & can out-last support ● May be formally designed, assessed & certified, making subsequent changes risky & costly ● Often specialised, custom-designed for particular purposes	● Many OT systems rely on 'legacy' platforms with infrastructure, hardware, software, protocol & process vulnerabilities ● Long, convoluted, international supply chains frustrate traceability, security & assurance ● Having been designed for resilience, changes to OT systems are risky, physically demanding, costly & blocked/avoided, since service interruptions—even for planned maintenance & upgrades— are unacceptable ● OT-specific risks include tampering, vandalism & sabotaging machinery, monitoring & control equipment, & production, theft of intellectual property, proprietary control programs & parameters, physical equipment degradation, storms, fires, floods *etc*. ● Incidents may have serious or catastrophic safety consequences such as explosions, loss of control of manufacturing plant & machinery, chemical releases & environmental disasters, while incidents affecting critical infrastructure can cause chaos ● *Significant* threats relating to geo-politics, military action, commercial disputes, terrorists, activists *etc*. taking an interest in the festering cluster of OT vulnerabilities & potentially devastating impacts of major OT incidents on national infrastructure	● Systems explicitly "over-engineered" for availability & resilience *e.g.* physically strong materials & enclosures, redundancy, automated fail-over, reliable recovery mechanisms … ● Systems explicitly engineered for safety *e.g.* formal designs, explicitly-defined limits, layered controls, lockouts … ● The usual range of security controls *e.g.* policies, procedures, access controls, cryptography, backups, change controls, incident management *etc*. gradually being introduced (despite persistent legacy issues) ● Strong assurance *e.g.* safety & security certification, pentesting, audits, exercises … ● Obscurity – a weak fail-unsafe control ● Proactive monitoring, especially for availability & safety, with strong alarms, logging & some automated responses ● Well designed & practiced event, incident & emergency responses with coordination & collaboration among emergency services ● Information sharing among intersecting communities of interest

Tech domain	Characteristics & features	Information risks	Security controls
Mobile (MT)	● Ad hoc wireless networks using various protocols & frequency bands ● Small, cheap IoT *things* are proliferating ● Some are wearable or implantable ●	● Some dependence on communications infrastructure & security, although network connections may span insecure or untrustworthy nodes or areas ● Physical device security cannot be guaranteed, even with tamper resistance ● Reliably identifying & authenticating devices & users can be challenging, especially in the case of cheap consumer-grade *things* expressly designed for low cost - not security, quality, privacy, safety, maintainability, longevity *etc*.	● Cryptography to protect network communications ● Powered by batteries, some with solar cells or generators, giving less reliance on the electricity grid & greater resilience to power cuts ● Evolving security standards, assurance & labelling schemes
Virtual (VT)	● Software-defined ● Complex ● Dynamic ● Abstraction layers ● Cloud! ● Agility ● Scalability	● Complexity + dynamics + cutting edge = risky ● Enterprise systems on shared infrastructure, often separately owned & controlled ● Virtualisation/emulation is *faking* reality ● Tenants compromisable via the virtualisation layer or host/shared services, plus social engineering of data centre & security staff ● Heavy trust in the technology ● Systems heavily loaded running hot	● High quality facilities designed & managed for security ● Systems & services designed for isolation ● Automated dynamic reallocation of resources - flexible, cost-effective ● Good BCP/DR/resilience, high uptime ● Automated system & security monitoring, administration & responses
Smart (ST)	● All forms of **A**rtificial **I**ntelligence ● Smart devices, systems, services, cities, vehicles, organisations … ● Systems-of-systems that form, communicate, collaborate & act collectively in real time ● Capable of rapid responses to complex situations involving voluminous information	● IT+OT+VT risks, for starters (see above!) ● Opaque internal automated processes ● Learning systems are self-reprogramming, adapting in ways that may not be entirely predictable & controllable ● Intense commercial rivalry & rapid technological advancement ● Smart offence (escalating cyberwar)	● ?? This is an immature developing field. ● For now, conventional security controls are being applied, perhaps not consistently & with challenges relating specifically to AI *e.g.* limited change controls, weak assurance ● Potential & need for smart automated defence – detection, decisions, responses …