Appendix 7. Glossary

Alt Text	Brief description of an image to help with searching
APT	Advanced Persistent Threat
IoT	Internet of Things, a collective network of connected devices and technologies that facilitates communication between devices and the cloud and also between the devices themselves
Kill Chain	In cybersecurity, the term Kill Chain describes the sequence of steps that cybercriminals go through when attempting to carry out a successful cyberattack
LMS	Learning Management System
MOOC	Massive Open Online Courses, a modern form of distance education
ROI	Return on Investment ratio, which helps calculate the return on investment in a project
XDR	Extended Detection and Response, a class of information security systems for the extended detection and response to complex threats and targeted attacks
Additive technologies	A method of creating three-dimensional objects, parts, or things by adding material layer by layer
APCS	Automated process control system
Builder	A tool that can configure the parameters of malware before using it in a cyberattack
Endpoints and end devices	Physical devices that connect to and exchange data with a computer network (mobile devices, desktop computers, virtual machines, embedded hardware, or servers)
Neuromorphic processor	A processor whose functional principle and architecture are similar to the neural networks of living organisms
GG	Greenhouse gases and gaseous substances of natural or manmade origin that absorb and re-emit infrared radiation
Reverse engineering	Reverse engineering is the process of analyzing the machine code of a program in order to understand the principle of operation, restore the algorithm, discover undocumented program capabilities, etc.
MDR solutions	Managed Detection and Response solutions for the automatic detection and analysis of security incidents in infrastructure using telemetry and advanced machine learning technologies
Technical attribution	The process of determining or uncovering identification information that can identify or link a specific attacker, group of attackers or source country to a specific cyberattack or cyber incident
Unique user	A user who visited an Internet resource within a certain period of time (usually within 24 hours)
Data exfiltration	The process during which an attacker extracts sensitive data from another computer's system and uses it for personal gain