**Week 6 Overview: The Future of the Internet & Generative AI**

This week brings together everything you’ve learned throughout the module to **explore the future of the internet**, considering **technological, security, legal, social, and privacy challenges**. You will also examine **generative AI** and its potential impact on network security through research, debates, and collaborative activities.

**Key Learning Areas**

**1. The Future of the Internet**

* Review how current internet technologies face **security, privacy, and performance limitations**.
* Explore **next-generation internet solutions** that aim to overcome these issues, including:
  + **Software-Defined Networking (SDN)** and its role in improving efficiency and security (*Rawat & Reddy, 2017*).
  + New internet architectures designed with **security and privacy as core principles** (*Ding et al., 2016*).
  + Alternative approaches like **ID/Locator split architectures** for future network design (*Shaotong, 2016*).
* Understand how these innovations **address modern challenges**, such as:
  + Cyberattacks and data breaches.
  + Legal compliance, including **GDPR**.
  + Protecting user privacy and organizational data integrity.

**2. Generative AI and Network Security**

* Explore how **Generative AI (GenAI)** is changing the cybersecurity landscape:
  + Automating threat detection and response.
  + Identifying vulnerabilities faster than traditional methods.
  + Supporting human analysts with advanced insights.
* Debate the **benefits and risks** of AI in cybersecurity:
  + **Benefits:** Faster, more accurate threat detection and patching vulnerabilities.
  + **Risks:** Overreliance on AI, adversarial attacks, and manipulation by hackers.
  + **Human vs. AI balance:** Deciding where automation ends and human expertise begins.

**Seminar activity:**  
Work in teams to present arguments for and against generative AI in network security.  
Each team will create a **PowerPoint presentation**, then vote on the most persuasive argument.

**3. Pulling Together Findings – Executive Summary**

* Complete an **executive summary report** (1,200 words, 40% of your grade) that builds on your earlier work from Unit 3.
* Report must include:
  1. A **summary of all work done**, including key findings.
  2. Clear, **non-technical results** supported by visuals like charts or graphs.
  3. **Evaluation against two security standards**, one of which must be **GDPR**.
  4. **Recommendations**, prioritized by business impact and compliance requirements.
  5. Clear **conclusions** tied back to data and analysis.

**4. Final Reflection on Learning**

* Create a **reflective piece** (800 words or a video diary, 30% of your grade) documenting your growth and learning throughout the module.
* This includes:
  + Your experiences with key topics such as breaches, vulnerability testing, logging, and AI.
  + Challenges you faced and how you overcame them.
  + Insights into **legal, social, ethical, and professional issues** in cybersecurity.
  + Skills you’ve developed, such as critical thinking, problem-solving, and digital literacy.

You may use **Rolfe et al.’s (2001) model**:

* **What?** – Describe what happened or what you learned.
* **So what?** – Explain why it matters and its significance.
* **Now what?** – Show how you will apply this learning in future scenarios.

**Formative Activities**

* Attend and prepare for the **Generative AI debate seminar**.
* Update the **Module Wiki** with final insights and key terms.
* Continue gathering data and feedback to support your final assignments.

**Learning Outcomes by the End of Week 6**

By the conclusion of this module, you will be able to:

1. **Describe next-generation internet technologies** and how they address technical and security challenges.
2. **Debate and critically assess** the role of generative AI in network security.
3. **Evaluate and compare systems against modern security standards**, including GDPR.
4. **Produce professional-level reports** and actionable recommendations for businesses.
5. **Reflect on your personal development**, skills growth, and professional readiness as a cybersecurity practitioner.

**Why Week 6 Matters**

* Brings **theory and practice together**, preparing you for real-world cybersecurity roles.
* Encourages **forward-thinking** about the future of the internet and the role of AI in security.
* Strengthens **presentation, reporting, and reflective skills** essential for ongoing professional development.

**In summary**, Week 6 challenges you to think critically about the **future of network security**, apply your knowledge to **emerging technologies**, and demonstrate your skills through high-level analysis, collaboration, and reflection.