CoGrammar

Welcome to this session:

Open Session:

Enhancing Infrastructure Security in Response to Russian Naval Activities

The session will start shortly...

Any Questions?
Drop them in the questions section.

Safeguarding & Welfare

We are committed to all our students and staff feeling safe and happy; we want to make sure there is always someone you can turn to if you are worried about anything.

If you are feeling upset or unsafe, are worried about a friend, student or family member, or you feel like something isn't right, speak to our safeguarding team:

Ian Wyles
Designated Safeguarding Lead

Simone Botes

Nurhaan Snyman

Rafiq Manan

Ronald Munodawafa

Tevin Pitts

Scan to report a safeguarding concern

or email the Designated Safeguarding Lead:
Ian Wyles
safeguarding@hyperiondev.com

CoGrammar   HyperionDev

HOUSEKEEPING

Leadership & Management Live Lectures – Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment for all - please engage accordingly.

    - *(Fundamental British Values: Mutual Respect and Tolerance)*

- No question is daft or silly - **ask them!**

- Should you have a question during the lecture, please feel free to **post in the Questions section** and I will respond throughout.

CoGrammar

Leadership & Management Live Lectures – Housekeeping

- Activating **live captions** in your browser's accessibility settings is a helpful option for better understanding, especially for those with hearing impairments or challenges with accents.

- For all **non-academic questions**, please submit a query: **www.hyperiondev.com/support**

- Report a safeguarding incident: **www.hyperiondev.com/safeguardreporting**

- Should you have any further questions or want to provide us with feedback, please feel free to post them **here.**

- **GitHub Link to access L&M Presentation Slides.**

PLEASE NOTE...

CoGrammar

LEARNING OBJECTIVE

Learning Objective

Understand how to use **Idea Management, and Specification** to develop innovative solutions for **safeguarding critical infrastructure**, such as undersea cables.

WELCOME

CoGrammar

*Leadership & Management/**Open Session***

In April 2024, reports of **Russian spy ships near the UK's critical undersea cables** raised alarms.

Why? These **cables carry 95% of global internet traffic**, making them vital to international communications and commerce.

WELCOME

Undersea cables are the unsung heroes of our digital age. These fibre optic cables, some spanning thousands of kilometers, rest on the ocean floor and connect continents, enabling everything from financial transactions to video calls.

Around £10 trillion in financial transactions flow through these cables every single day.

That's not just your Netflix binge or social media scrolling; that's global stock exchanges, critical banking systems, and even defence communications relying on these invisible threads under the ocean.

When a spy ship lingers near these cables, it raises two major concerns:

- **Espionage:** Nations **could intercept sensitive data** flowing through these cables, gaining access to confidential communications.

- **Sabotage:** A severed or damaged cable **could disrupt internet access, causing widespread economic and social chaos**. For example, in 2021, a single damaged cable disrupted internet services across parts of Africa for weeks.

The situation is further complicated by the sheer **vulnerability of these cables**. Most are unprotected and lie on the seabed without significant physical security measures.

Recent reports from the UK Ministry of Defence have **underscored the need for greater protection**, particularly given geopolitical tensions.

WELCOME

Why is this so alarming for the UK?

- The UK is a hub for undersea cable landings, making it a **crucial node in the global internet network**. An attack or breach here would ripple through Europe, North America, and beyond.

- During the **Cold War, similar activities were conducted** by the US and Soviet Union, where nations attempted to tap or disrupt cables for strategic advantage. Now, with the stakes even higher in our digital world, these threats feel more immediate and real.

WELCOME

Call to Action for Students

As emerging leaders in your fields, **understanding the vulnerabilities** of critical infrastructure is essential. Think about this:

"How can we innovate to protect these cables? Could there be ways to monitor activity around them, enhance physical protection, or encrypt data to make espionage less feasible?"

CoGrammar

RESPECT

The UK, a global hub, collaborates with other nations to **uphold the integrity of international communication**.

IDEA MANAGEMENT

CoGrammar

IDEA MANAGEMENT

Idea management is the **process of collecting, refining, and selecting the best ideas** to solve challenges or drive innovation.

CoGrammar

IDEA MANAGEMENT

Norway's Undersea Cable Protection: Seabed Sensors

Technology Deployed: Implemented advanced seabed sensors to monitor the physical integrity of cables. These sensors detect unusual activities, such as tampering or proximity of unauthorised vessels.

Integration with National Security: Part of a broader maritime surveillance system that collaborates with its naval forces, ensuring quick response to any threats.

Outcomes: Norway's model showcases the importance of blending technology with real-time actionable intelligence.

CoGrammar

IDEA MANAGEMENT

Australia's Use of Submarine Drones for Surveillance

Key Features: These autonomous underwater vehicles (AUVs) are equipped with advanced cameras and sonar systems, capable of monitoring cables for signs of damage or interference.

Versatility: Operate across varying depths and terrains, making them suitable for both shallow and deep-sea cable protection.

International Collaboration: Australia has integrated these technologies into joint efforts with allied nations, emphasizing the importance of collective action in securing global communications.

CoGrammar

RULE OF LAW

The implementation of protocols, legal frameworks, and technology deployments, such as submarine drones or seabed sensors, **adheres to international laws and treaties to maintain fairness and order**.

SPECIFICATION DEVELOPMENT

CoGrammar

*Leadership & Management/**Open Session***

SPECIFICATION DEVELOPMENT

Considerations when designing a system to detect undersea cable interference

- **Reliability:** How can we ensure uninterrupted data flow?

- **Real-Time Alerts:** What system could notify stakeholders of tampering immediately?

- **Cost-Effectiveness:** What is a sustainable budget?

- **Environmental Impact:** How do we minimize disruption to marine life?

CoGrammar

SPECIFICATION DEVELOPMENT

NATO's Maritime Security Framework

Outlines a comprehensive **strategy for protecting critical maritime infrastructure**, including undersea cables, recognising the increasing geopolitical and economic importance of maritime domains.
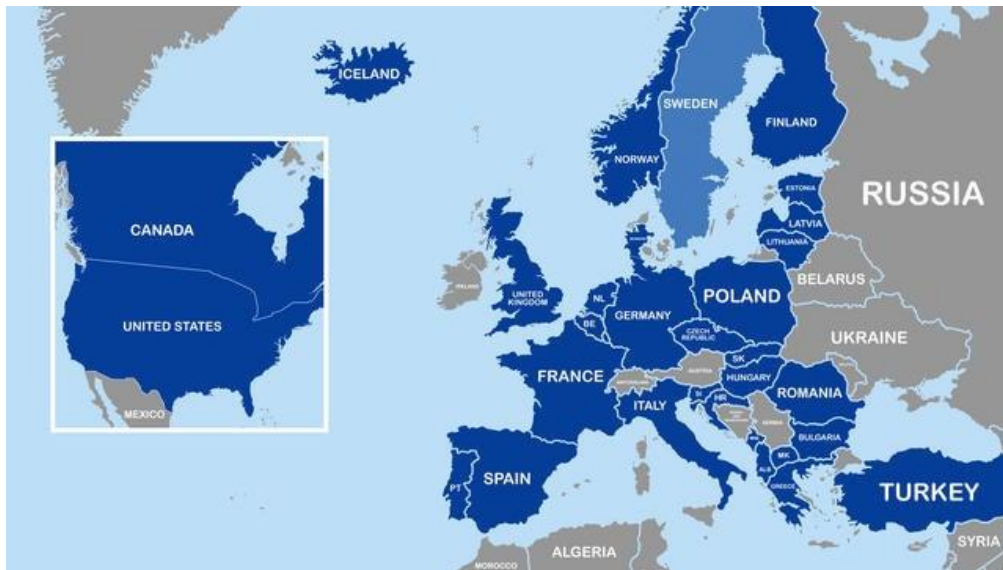
©CBS

SPECIFICATION DEVELOPMENT

NATO's Maritime Security Framework

- **Key Focus:** The framework **emphasizes the need for multi-layered defence strategies**, incorporating advanced surveillance technologies, risk assessment protocols, and robust international collaboration.

- **Rationale:** As 95% of global internet traffic relies on undersea cables, any disruption to these assets could have far-reaching consequences for global commerce, communication, and security.

CoGrammar

NATO's Maritime Security Framework

Surveillance

NATO prioritises continuous monitoring of maritime domains through integrated surveillance systems, including satellite imagery, sonar detection, and maritime patrols.

SPECIFICATION DEVELOPMENT

NATO's Maritime Security Framework

Risk Assessment

Regular threat evaluations and vulnerability assessments of undersea cables and maritime assets are essential to stay ahead of potential disruptions or sabotage attempts.

NATO encourages member nations to share intelligence to better anticipate and mitigate threats.

CoGrammar

SPECIFICATION DEVELOPMENT

NATO's Maritime Security Framework

International Collaboration

Recognising the transnational nature of maritime security, the framework emphasizes joint efforts among NATO allies.

Initiatives include conducting joint naval exercises, establishing shared communication protocols, and promoting standardised maritime security practices.

Collaboration extends beyond NATO members to include partners such as the EU and like-minded nations.

Relevance to Undersea Cable Security

The **Maritime Security Framework provides a blueprint for safeguarding undersea cables** through its emphasis on:

- **Layered Security:** Combining advanced technologies like drones, sensors, and naval patrols to create overlapping defences.

SPECIFICATION DEVELOPMENT

Relevance to Undersea Cable Security

- **Collaboration:** Strengthening alliances and partnerships to respond to shared threats.

- **Adaptability:** Encouraging innovation to address emerging challenges, such as cyber-attacks on maritime systems or sabotage by state and non-state actors.

DEMOCRACY

The inclusivity of NATO's framework, which **encourages member nations to share intelligence and collaborate**, reflects democratic principles of shared governance and decision-making.

THE END
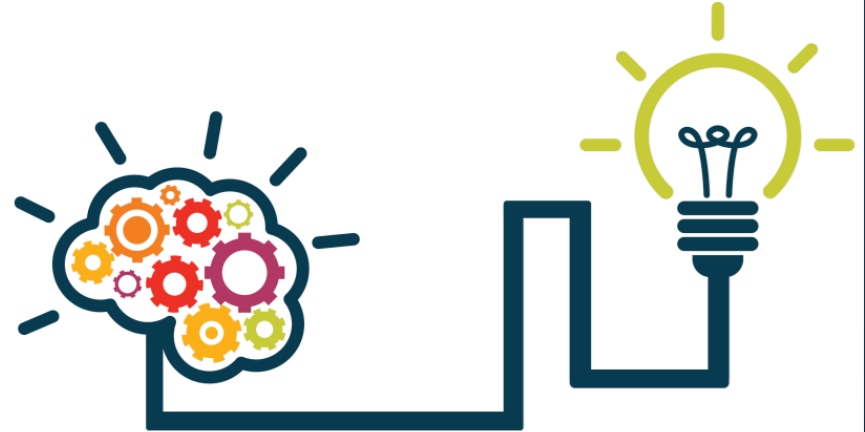
CoGrammar

*Leadership & Management/**Open Session***

CONCLUSION

Key Points

Idea Management: Gather and refine innovative ideas.

Specification Development: Clearly define requirements.

RESOURCES

RESOURCES

Articles

- ✓ **UK monitors Russian spy ship, steps up undersea cable protection**

- ✓ **Russian spy ship escorted away from area with critical cables in Irish Sea**

- ✓ **NATO's maritime activities**

- ✓ **National Cyber Strategy 2022**

Thank you for attending

CoGrammar

SKILLS FOR LIFE — SKILLS BOOTCAMPS | Department for Education