GROUPE E - CYBER-ATTACKS (Section 5)

STEP 1: UNDERSTAND YOUR SECTION

Answer these questions:

1. **Main question:** Can AI now carry out fully autonomous cyber-attacks?

   → Answer: _______ (yes/no/not yet)

2. **What AI CAN do: AI systems can support cyber-attackers at various stages. List the 3 stages mentioned:**

……

3. **What AI CANNOT do yet:** Why can't AI carry out fully automated attacks?

   → Because AI cannot yet execute ____________________________ tasks.

4. **Why this matters:** If AI could do fully automated attacks, what would happen?

   → Criminals could launch attacks on a far _________ scale.

5. **Real example - Claude Code:**
   - Who used it? A **-** group from __________________
   - How many entities attacked? __________________
   - Success rate? "a __________________ of successful __________________ "
   - Percentage performed without human intervention? _______% to _______%

6. **Key term:** What does "a high degree of autonomy" mean?

……

……

7. **Why is this example important?** What does it show about the future of cyber-attacks?

……

……

8. **Your analysis:** In YOUR future job (cybersecurity), how will AI change:
   - The work of attackers? ____________________________________
   - The work of defenders (you)? ____________________________________

   Your general opinion on AI and cybersecurity

……

……

……

……

……

STEP 2: RESEARCH

Your task: Find current information about AI in cybersecurity

What to search for:

- AI tools for cyber-attacks (examples, techniques)
- AI tools for cyber-defense (SIEM, threat detection)
- Recent cyber-attacks using AI
- How cybersecurity professionals use AI

Suggested searches:

- "AI cybersecurity attacks 2025"
- "AI threat detection tools"
- "autonomous cyberattacks examples"
- "AI SIEM Splunk Darktrace"

Take notes –

Source (website/video)	Date	Main information	How it connects to your section

STEP 3: PREPARE PRESENTATION

Introduction (30 sec):

- Topic: AI and cyber-attacks - are they autonomous yet?
- **Why this is crucial for YOUR future career**

Main points (2 min 30 sec):

- What AI can do: support at various stages
- What AI cannot do yet: fully autonomous multi-stage attacks
- Claude Code example (Chinese attack, 80-90% autonomous)
- Why this matters: scale of attacks could increase dramatically

Your research (1 min):

- Example of AI attack tool OR AI defense tool
- **Technical explanation** (use your CIEL knowledge!)

Debate question (30 sec):

- "Should AI coding tools like Claude Code be restricted to prevent cyber-attacks?"

DEBATE QUESTIONS - PREPARE TECHNICAL ANSWERS

1. If 80-90% of a cyber-attack can already be automated, what's the impact on:
   - Number of attacks?
   - Types of companies targeted?
   - Your future job as cybersecurity analyst?
2. Should companies like Anthropic be held responsible if their AI tools are used for attacks?
3. **Technical question:** How can AI help DEFEND against cyber-attacks? Give concrete examples.
4. In 5 years, will attackers or defenders have the advantage with AI? Why?