Round Table Cyber InSecurity?

Stage1: Prepare a Lead-in

Choose the case you would like to use in the lead-in as an introduction into the matter. These could be the most daring cyber attacks, notorious data thefts, sensational leaks. The lead-in is down to the moderator, but the discussion stage is to be done as a group. Google Docs will come in handy when you need to share your findings with the other team members.

Stage 2: Topic-related vocabulary

While preparing for the round table, you will be reading articles on the subject and watching related videos. Whenever you come across a word or a collocation pertaining to the topic (within the topic of cyber security these could be words and phrases like *firewall*, *large-scale targeted intrusion*, *pwn*, E2EE (*end-to-end encryption)*, etc.), write it down in your topic vocabulary list. This is best done at Google Docs, where you group all of your findings in a table, as shown in the example below.

Name	Word/collocation	Definition	Example
Student 1	-	-	-
Student2	-	-	-

In order to have a clear understanding of when and how these new words and phrases can be used, please, consult the English language corpora online, following the links below. (A corpus is a compilation of authentic written and spoken language, which enables learners to trace patterns of grammar and vocabulary usage)

https://www.english-corpora.org/bnc/

https://www.english-corpora.org/coca/

Stage 3: Define perspectives for the discussion

At this stage, students do not assume roles yet, they rather speculate on the variety of opinions that could be voiced on the subject and do Internet and other media research.

It is better if the number of perspectives equals the number of attendees, which does not exclude the possibility of some of the speakers having points of convergence.

Here are some examples of the perspectives on Cyber security and Cyber Threat

- Cyber security is not only the matter of concern for businesses and states; the safety of regular citizens is at stake.
- Individuals had better forgo their right to privacy to safety.
- Cyber war can be as detrimental to the economy of a country as a traditional one.

Report on your progress in class.

Stage 4: Assume roles and prepare for the role-play

Choose a public figure whose views you would like to present and prepare a set of arguments to support your stance. This task requires both analytical and critical skills.

- **Chairperson** makes an opening statement and offers a lead-in, sets the tone of the discussion focusing on the following questions
- How can cyber security be promoted at different levels - that of individuals, businesses, states, the whole world?
- Does weakening encryption* entail infringement on personal freedoms?
- What could be the consequences of cyber war and how can it be prevented?

The list of questions and points for discussion is to be continued by the student that assumes this role (use Google Docs).

- **Edward Snowden**, American whistleblower, former NSA officer, claims that without encryption we will lose all privacy

https://www.theguardian.com/commentisfree/2019/oct/15/encryption-lose-privacy-us-uk-australia-facebook

For more information on Edward Snowden you may want want to watch the film *SNOWDEN*

- **Crispin Robbins**, GCHQ's** technical director for cryptanalysis. Privacy and security protections are critical to public confidence. Therefore, we will only seek exceptional access to data where there's a legitimate need, that access is the least intrusive way of proceeding and there is appropriate legal authorisation.

https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate

- **Ian Levy**, technical director for GCHQ's National Cyber Security Centre, co-author of the proposal to provide 'back doors' for the law enforcement agencies. Claims that their aim

is not to weaken encryption as such, but to add ‘a secret eavesdropper’ to chats and conversations. The proposal was met with criticism from the major tech giants and human rights activists as the one which undermines credibility in social media.

https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate

- **Mark Zuckerberg,** Facebook CEO defends the decision to encrypt the company’s messaging services despite the concerns that such encryption may facilitate criminal activity online, such as child exploitation, terrorism, etc.

https://www.telegraph.co.uk/news/2019/10/04/facebooks-zuckerberg-defends-decision-encryption/

https://www.cyberscoop.com/gchq-encryption-letter-going-dark/

The house giants wrote an open letter in response to the initiative of Robbins and Levy

https://newamericadotorg.s3.amazonaws.com/documents/Coalition_Letter_to_GCHQ_on_Ghost_Proposal_-_May_22_2019.pdf

- **Megyn Kelly,** American journalist, interviewed Vladimir Putin in 2017, persists with the claims that Russian hackers meddled in the US 2016 elections

https://www.nbcnews.com/news/world/vladimir-putin-faces-questions-megyn-kelly-st-petersburg-n767481

- **Oleg Demidov,** consultant on legal regulation in cyber security in the UN Institute for Disarmament Research. Despite the mutual accusations of cyber attacks, U.S.-Russia cyber negotiations could still be successful.

https://eng.globalaffairs.ru/book/Increasing-International-Cooperation-in-Cybersecurity-and-Adapting-Cyber-Norms-19391

https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms

https://www.pircenter.org/en/experts/13-demidov-oleg-v

- **Klon Kitchen,** leads tech policy at the Heritage Foundation. Cyber threat is underestimated, especially economy-wise

https://www.heritage.org/cybersecurity/commentary/major-threat-our-economy-three-cyber-trends-the-us-must-address-protect

- **Sarah Stephens,** cyber, media and technology leader in the UK financial and professional practice at Marsh JLT Specialty. Cyber attacks could be more costly than natural disasters, such as Sandy Storm, so a suitable insurance policy should be tailored for each and every enterprise

https://www.sciencedirect.com/science/article/abs/pii/S136137232030018X

https://www.ft.com/content/dff0649c-671a-11e7-8526-7b38dcaef614

**encryption* of messages on social media and messengers grants privacy to participants of online chats. Neither individuals nor government bodies can access these conversations even if they suggest criminal activity.

**_GCHQ_ - Government Communications Headquarters is an intelligence and security organisation responsible for providing signals intelligence (SIGINT) and information assurance to the government and armed forces of the United Kingdom. Based in "The Doughnut" in the suburbs of Cheltenham, GCHQ is the responsibility of the country's Secretary of State for Foreign and Commonwealth Affairs, but it is not a part of the Foreign Office and its director ranks as a Permanent Secretary. (Wikipedia)

Both representatives of this organisation, Crispin Robbins and Ian Levy, share a similar attitude towards weakening encryption and providing 'back doors' for intelligence services and law enforcement agencies

*** *going dark*

The term has been adopted by law enforcement to describe digital communication that cannot be monitored because of strong encryption. Mobile apps that use end-to-end encryption (E2EE) are designed to protect data at rest and in transit and keep the end user's text messages, emails and video chats private and secure. The same encryption technologies that protect end users from intruders, however, can prevent law enforcement and government agencies with the legal right to monitor transmissions from being able to do so. (https://whatis.techtarget.com/definition/going-dark)

Stage 5: Roleplay the round-table discussion in class