Seminar Series Misinformation Disinformation – Meeting Minutes

Format:	Expert Talk
Moderators:	Major Baur
Experts:	Mr. **Doowan Lee**, Founder & Chairman of VAST-OSINT, Senior Advisor in IST, and adjunct professor of politics at the University of San Francisco Lieutenant Colonel **Caspar Versteegden**, Teacher of International Security Studies at the Royal Netherlands Defense Academy Mr. **Jakub Kalenský**, Senior Analyst, The European Centre of Excellence for Countering Hybrid Threats Ms. **Katarína Klingová**, Senior Research Fellow, Centre for Democracy & Resilience, GLOBSEC
Audience:	Open to the public. Practitioners, experts, academics, and advanced students
Date:	16 Nov 22, 14:30 - 17:00 UTC+1
Duration:	150 min

Guiding Questions:

- What characterises Misinformation and Disinformation, and what are the differences in their appearance in traditional and social media?

- What is the risk of Misinformation and Disinformation to emerge in research, and what techniques to put in place to mitigate pitfalls?

- How will Civil-Military Cooperation and Civil Affairs have to adapt to the consequences arriving from the strategic, operational and tactical use of Disinformation?

Expert: Mr. Doowan Lee
Title: The Disinfo Ecosystem & CPD Strategies

→ Mr. Lee's lecture wanted to point out how disinformation evolved in the past 10 years. Such evolution was so rapid, thanks to the latest progress in technology, that it is crucial to understand what kind of variance we have seen in the past few years because it's impossible to apply all tools to detect and counter new threats.

1. Examining the Assumptions about Disinformation

    - Disinformation it's a broad problem that now, in the digital era, found in social media a primary environment to develop in.

    - Bad actors are ideologically or culturally driven: most of them disseminate misleading content just to generate traffic or garner attention. The problem is not on an individual level but on a systemic one since it incentivizes the proliferation of clickbait content.

- Bad content it's not to blame only for its untruthfulness but rather for its speed of amplification.

- Domestic bad actors support bad regimes. Nevertheless, defining all the unwitting actors as malign could be dangerous, sometimes domestic actors just amplify any content that is compatible with their belief system.

- Fact-checking and debunking work best against disinformation (more truthful content wins). However, they can not compete with a more scalable resilience and upstream detection and prevention.

2. The Flawed Incentive of Content Propagation
    I. The Vast Content Ecosystem: A Supply Chain Approach

        - disinformation in its composition
        - origins of disinformation

    II. Nodes Diagram

        - Network Analysis: a fragment of Data Analysis (50'000 unique domains) all connected to amplify the Kremlin's disinformation about the war in Ukraine. Compared to manual analysis, network analysis is much deeper and broader.

    III. Conclusions

        - No events or stories are immune from mischaracterization and disinformation. The authoritarian regimes' content ecosystems are transnational and vast.
        - Information pollution has become "democratized". That is, it's become so cost-effective, lucrative, and widely available to use disinformation.
        - Only early detection and proactive engagement at scale seem to work to compete effectively in the information environment.

3. CPD Strategies

    - Deplatforming: Account/User Removal - highly pragmatic
    - Content Moderation/Removal - highly pragmatic, but who decide?
    - Awareness: Digital Literacy - depends on the scholarship of the country where is applied
    - Strategic Communications: Counter or Proactive Messaging - slightly pragmatic (takes a lot of resources)
    - Provenance: Exposing Content Origins & Quality at Scale - very important but not effectively put into practice yet
    - Content Validation: Fact Checking - often weaponized

Expert: Lieutenant Colonel Caspar Versteegden
Title: Resilience can counter Dezinformatsiya

→ Lieutenant Colonel Caspar Versteegden starts his presentation with a case study on the flight MH-17 tragedy in 2014 and the disinformation that has been done about it.

1. What is disinformation and why is it used

    - purposeful spreading of diverging and confusing theories through various channels to create information overload
    - Russian Reflexive Control Theory
    - generate chaos to keep western influence away from its borders

2. How resilience can be supportive against disinformation

    - strengthening of social cohesion leading disinformation to be questionate
    - building of trust in institution by constantly pointing out advantages of existing norms and values

3. How can resilience be enhanced

    - resilience building blocks: social capital, trust norm values, interconnectedness, innovation and education, awareness

4. Can resilience counter disinformation

    - specific resilience fundamental aspects can counter specific disinformation goals

5. Does Dutch, EU or NATO policy enhance Resilience

    - EU Strategic Compass - EU Hybrid Toolbox

6. Does the implementation of these policies work

    - study on NATO, EU, and The Netherlands

7. Proposal to enhance resilience

    - enhance trust

Expert: Mr. Jakub Kalenský
Title: Russia Disinformation: What it is and what makes it a threat

1. What is disinformation

- "False information with the intention to deceive public opinion."
  Great Soviet Enciclopedia, 1952
- Dis-information is both false, like Mis-information, and harmful, like Mal-information. It provides false context and imposter, manipulated, and fabricated content

2. Why do we cover Russian disinformation?

   - Globally, Russian FIEs cover 62% (the rest is accounted mostly to China, Iran, Saudi Arabia, and United Arab Emirates)
   - European authorities attribute 80% of influence efforts to Russia

3. What is Russia trying to achieve

   - Was decided by the European Commission's contribution to the European Council in the Action Plan against Disinformation in 2018
   - Information is one of the most important battlefields on which modern wars are fought

4. What makes it a threat

   - disinformation is a non-military measure for achieving military goals, as understood by both the authorities and the representatives of pseudo media
   - zero-sum game is the objective Russia would like to achieve

5. Narratives targeting Ukraine
   → to justify Russia's crimes in Ukraine

   I. The victim is the aggressor, the aggressor is the victim
      - Dehumanization of Ukraine
      - Identification of Ukrainians as Nazis or Fascist
      - Ukraine commits genocide and wages a civil war, especially against RU speakers
      - Ukraine is the West's launch pad for invading Russia

   II. Ukraine is worthless, governed by the West
      - Ukraine is a failed state: not a nation, not a country.
      - Ukraine is completely under the West's control

   III. Nuclear weapons
      - Ben Nimmo: "The 4D approach: Dismiss, Distort, Distract, Dismay
      - The nuclear threat against the opponents of the Russian invasions of Ukraine

6. Who is helping to achieve their goals

   - Not only a troll factory

- The ecosystem that spread RU disinformation

7. Four lines of defense

    - Documenting the threat
    - Raising awareness about the threat
    - Repairing the weaknesses in the information systems
    - Limiting, punishing deterring the information aggressor

Expert: Ms. Katarína Klingová
Title: Information operations in Central Europe

→ Central Europe and Disinformation, the Slovak case.

1. Actors
    - Foreign (Kremlin)
    - Domestic (political parties)
        - populistic and polarised narratives
        - network of amplifiers shows how detailed and well-connected the network of pro-Kremlin and disinformation in Slovakia is (timeframe one month and a half)
    - Low situational awareness of institutions undermines Resilience
    - Hungarian case
    - Covid-19: most of the conspiracy theory comes from the West
    - Night Wolves and Peter Švrček
    - Kremlin's machinery

2. Tools

    - Use of influencers and deep fake videos to spread particular narratives
    - 2014 video titled "Why does America needs a war in Europe" shows how sophisticated messages are
    - Mainstreamisation of disinformation (disinformation are becoming part of prime time political debates at mainstream media)
    - NATO StratCom CoE: monetisation of disinformation

3. Impact

    - GLOBSEC Trends 2022
    - Central Europe's perceptions of Russia
        - as a strategic partner
        - as a threat
        - as the cause of the war in Ukraine
    - Beliefs in conspiracy theories

Useful links and research proposed by experts:

- https://www.globsec.org/sites/default/files/2022-05/GLOBSEC-Trends-2022.pdf
- https://www.vulnerabilityindex.org/
- https://konspiratori.sk/zoznam-stranok/en
- https://time.com/6155060/lithuania-russia-fighting-disinformation-ukraine/
- https://www.globsec.org/sites/default/files/2020-10/Visualising_influence.pdf