

## CYBER OPERASJONER



## NORGE SINE SAMARBEIDSPARTNERE



#### **Group of Governmental Experts**

In GA resolution 73/266, the Secretary-General was requested to establish a Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security.

The GGE will also hold its first meeting in 2019 and is to submit its final report to the General Assembly in 2021. The group will be comprised of 25 members and its Chair will hold two informal consultations with all UN Member States in between its sessions. The mandate also includes consultations on the subject to be held with regional organizations, such as the African Union, the European Union, the Organization of American States, the Organization for Security and Cooperation in Europe and the Regional Forum of the Association of Southeast Asian Nations.

The Group of Governmental Expert comprises experts from 25 States working in their personal capacity. The Group has elected Ambassador Guilherme de Aguiar Patriota of Brazil to Chair the Group.

## NATO Cooperative Cyber Defence Centre of Excellence

CCDCOE

NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

The Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) is a NATO-accredited knowledge hub, think-tank and training facility. The international military organisation focuses on interdisciplinary applied research and development, as well as consultations, trainings and exercises in the field of cyber security. The Centre's mission is to enhance capability, cooperation and information-sharing between NATO, Allies and partners in cyber defence.



## TRUSLER FREM MOT 2030

### **TOP 10 EMERGING CYBER-SECURITY THREATS FOR 2030**

1 ∋8€

Supply chain compromise of software dependencies



Advanced disinformation campaigns



Rise of digital surveillance authoritarianism/ loss of privacy



Human error and exploited legacy systems within cyberphysical ecosystems



# EUROPEAN UNION AGENCY FOR CYBERSECURITY

10

Artificial Intelligence Abuse



THREATS 2030



Targeted attacks enhanced by smart device data



Lack of analysis and control of space-based infrastructure and objects

9

Cross border ICT service providers as a single point of failure



Skill shortage



Rise of advanced hybrid threats

## HVA BETYR ENDRINGER I TEKNOLOGI IHT SIKKERHET?

#### PERCEPTION LAYER

Large Data Volume,
Streaming Data Processing,
Lightweight Computation,
Decentralized Computation,
Composability,
Personalization.





#### **APPLICATION LAYER**

different types of privacy risks face data collected from users by applications they use.



#### **NETWORK LAYER**

Secure Communication, Anonymous Communication.

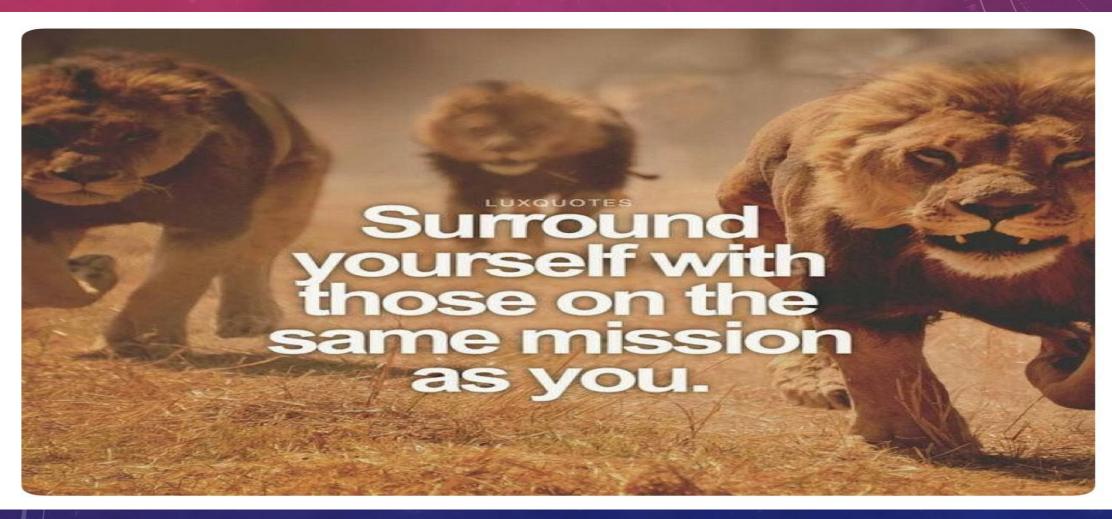




#### MIDDLEWARE LAYER

Interaction-Enhancing
Techniques, ComplianceEnhancing Techniques,
Evaluation of Existing
Middleware

# ER DET TRYGGEST Å LAGE SELV, ELLER BENYTTE FELLESLØSNINGER?

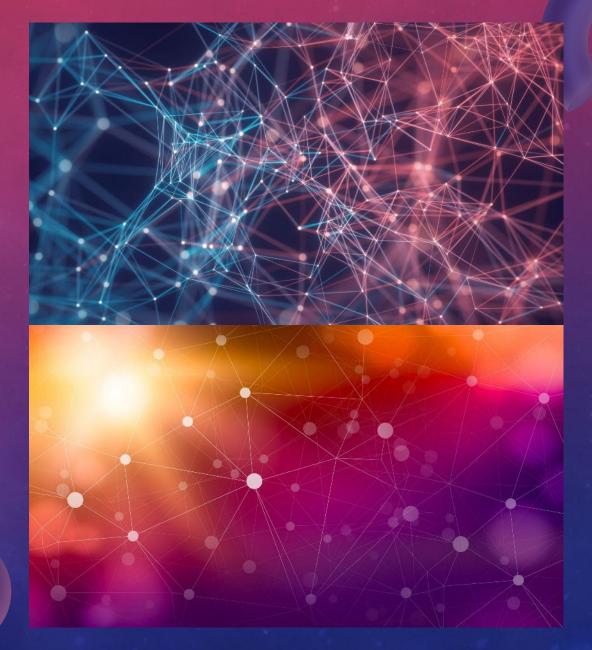


## TUSEN TAKK

Raymond Andre Hagen

Raymond.Andre.Hagen@digdir.no / raymohag@stud.ntnu.no

www.digdir.no / www.ntnu.no



Mandag 23.05.2022 8