

Electronic Toll Collection

Instrument Cluster

Head-Up Display

Wiper Control

Airbag Deployment

Electric Motor Management

Battery Management

Adaptive Front
Lighting

Night Vision

Driver Alertness Monitor

Accident Recorder

Event Data Recorder

Auto Dimming Mirror

Parental
Controls

Active Cabin Noise Suppression

Voice/Data Communications

Navigation System

Cabin Environment Controls

Entertainment System

Security System

Digital Turn Signals

Remote Keyless
Entry

Self-Parking
System

Project Lion Cage: Sikkerhetsdilemmaer ved programvare- styrte kjøretøy

Tor Indstøy – VP of Risk Management and Threat Intelligence, Telenor Group

Arild Tjomsland – Special Advisor TTO, University of Southeast Norway

Active Yaw

Adaptive Cruise Control

Automatic Braking (Brake-by-Wire)

Anti Lock Braking

Blind Spot Detection

Hill-Hold Control

Electronic Stability Control

Seat Position Control

Regenerative Braking

Tire Pressure Monitoring

Lane Departure Warning

Active Vibration Control

Active Suspension
Electric Power Steering



The Lion Cage Project

Førerassistentsystemer

- Drive-by-wire, steer-by-wire
- Kameraer, radarer, sensorer
- Skytjenester for navigasjon og talestyring
- OTA-plattformer → typegodkjenning blir tillitsbasert

Utstrakt bruk av skytjenester (delt mellom produsenter) for:

- Navigasjon
- Prosessering av talestyring
- OTA-plattformer for programvareoppdateringer

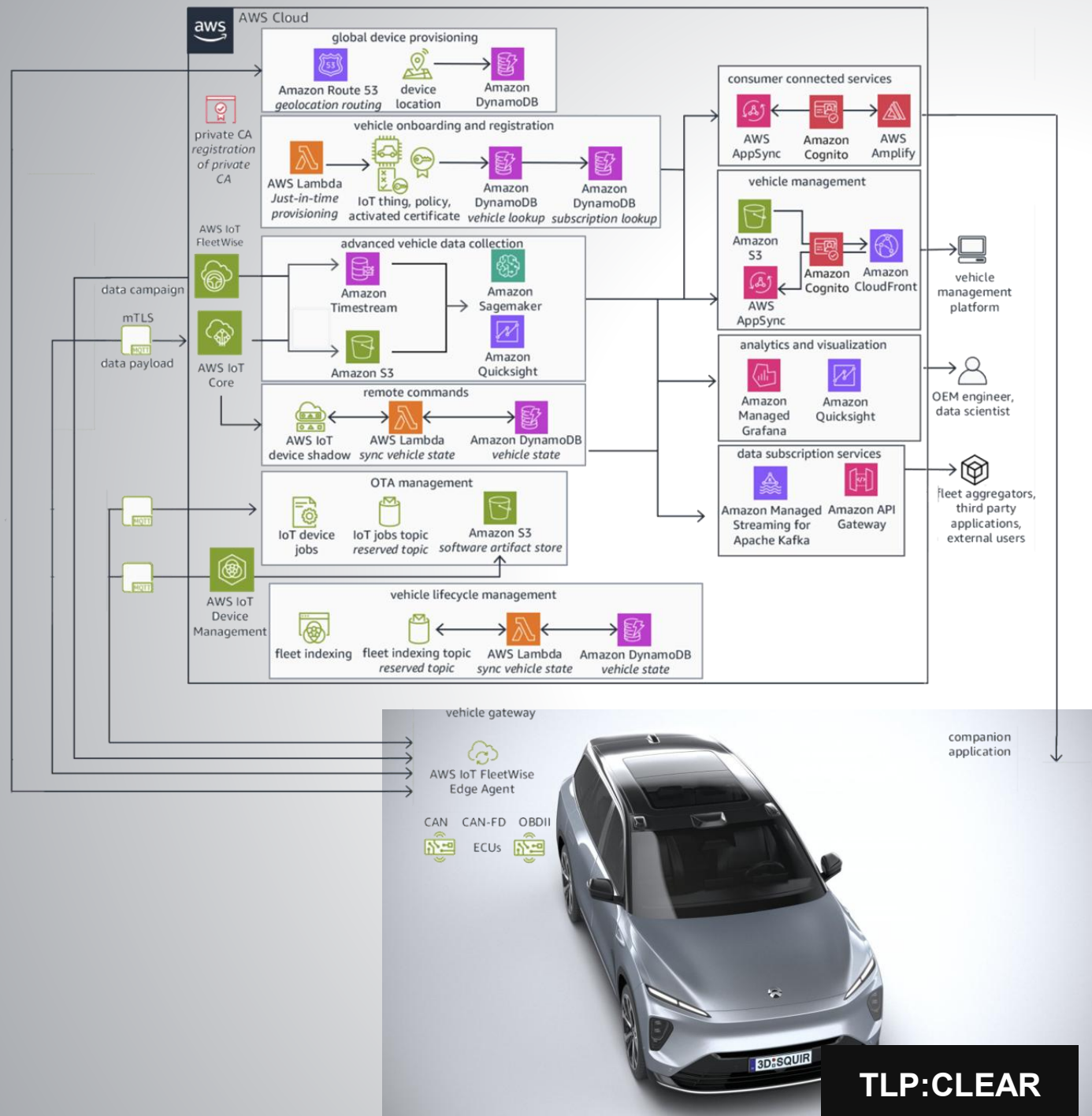
- Med OTA blir typegodkjenning tillitsbasert
- Cybersikkerhet for SDV-er er en prosess-sertifisering, uten testing av selve resultatet
- SDV-er er avhengige av produsenten for oppdateringer gjennom hele levetiden



Grensesnitt:

- Wi-Fi, mobilnett
- Bluetooth
- Ladeport
- Radio 315/433MHz
- Smartnøkkel/NFC,
- SOS-system
- GPS/GNSS
- CAN/OBD2
- Mobilapp
- Fysisk tilgang





Utfordringer:

- Sårbarhet for hacking
- Datainnsamling for samfunnsmodellering og AI
- Trafikksikkerhet og personlig sikkerhet
- Ansvarsproblemer – høy kompleksitet

• **Nasjonal sikkerhet**



SPIEGEL International



{ lat: 53.531474
lon: 10.371392

Volkswagen data breach raises important questions about how much information carmakers are collecting. Foto: [M] DER SPIEGEL; Fotos: Paul Langrock, Thomas Starck / AUTO BILD, picture alliance / dpa / Audi AG

We Know Where You Parked

Massive Data Breach at VW Raises Questions about Vehicle Privacy

Reuters

World ▾ Business ▾ Markets ▾ Sustainability ▾ Legal ▾ More ▾

Tesla workers shared sensitive images recorded by customer cars

By Steve Stecklow, Waylon Cunningham and Hyunjoo Jin

April 6, 2023 11:47 PM GMT+2 · Updated 2 years ago

Aa



TLP:CLEAR

Reuters

World ▾ Business ▾ Markets ▾ Sustainability ▾ More ▾

Norway says cyber attack on parliament carried out from China

By Nora Buli

July 19, 2021 10:48 PM GMT+2 · Updated July 19, 2021



DW



'No limits' to Russia-China ties

April 2025:

30 % av nye EV er kinesiske.



NIO ES8 for Oslo Taxi – 'et kjempekupp!'



NIO ES8 i bruk i selvkjørende pilot i Groruddalen, Oslo

Del 1

Teknisk sikkerhetsvurdering og risikoanalyse av Tor sin NIO ES8



Dere har kjørt kinesiske elbiler
inn i et fjell, og målt signalene den gir.



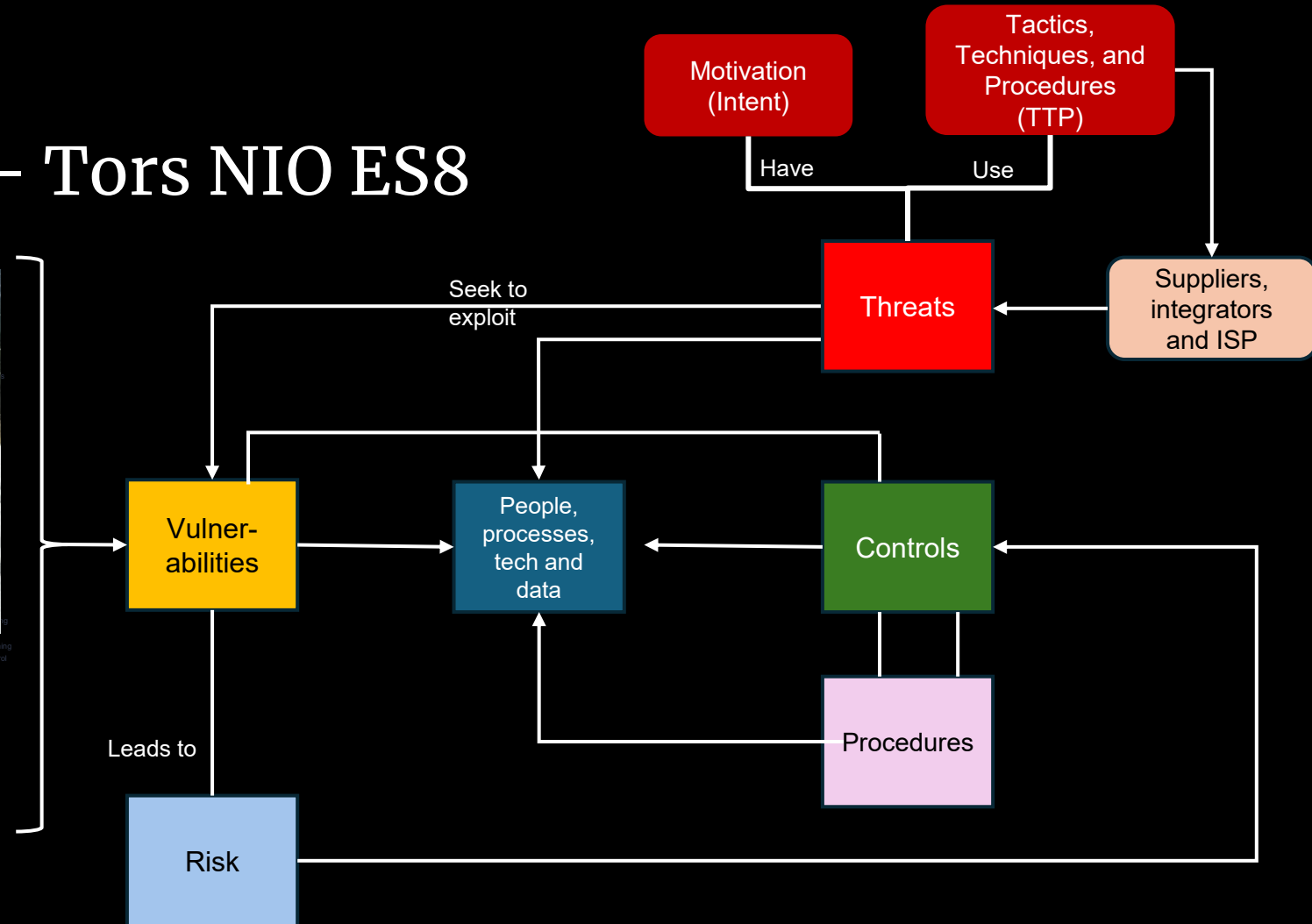
TLP: CLEAR

Del 1

Risikøkosystemet – Tors NIO ES8

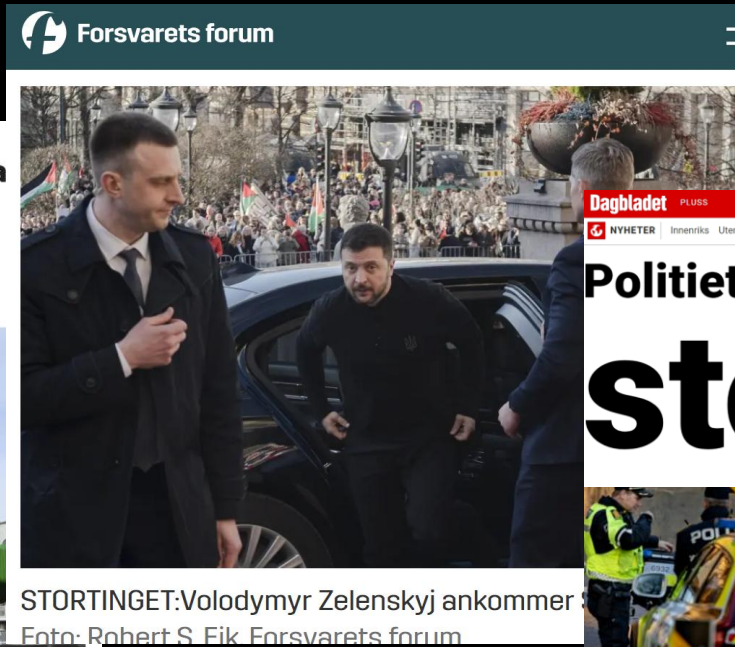


- Spektrumanalyse
- Bluetooth-sniffing
- Avlytting/oppsnapning av sender i bilen
- GPS-analyse
- Pentesting
- OSINT, inkludert: Patentanalyse / gjennomgang av patenter
- Kinesiske forum og meldingsplattformer



Scenariobasert tilnærming

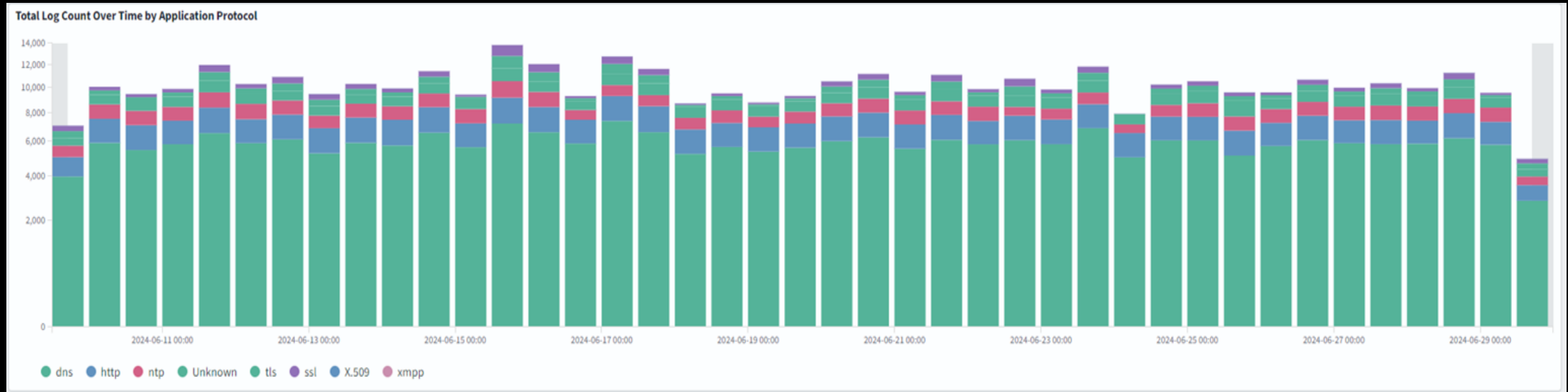
Scenario 1 – Trafikal sabotasje



Kan bilen til Tor brukes til trafikal sabotasje?



Funn: Bilen «skravler» kontinuerlig



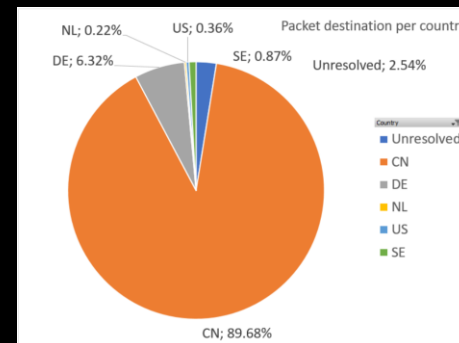
Datapakker går kontinuerlig inn og ut av bilen. Selv når bilen tilsynelatende er 'skrudd av'. Det er liten til ingen variasjon gjennom døgnet eller mellom geografiske områder.

70% av pakkene er kryptert, utstrakt bruk av ukjente protokoller

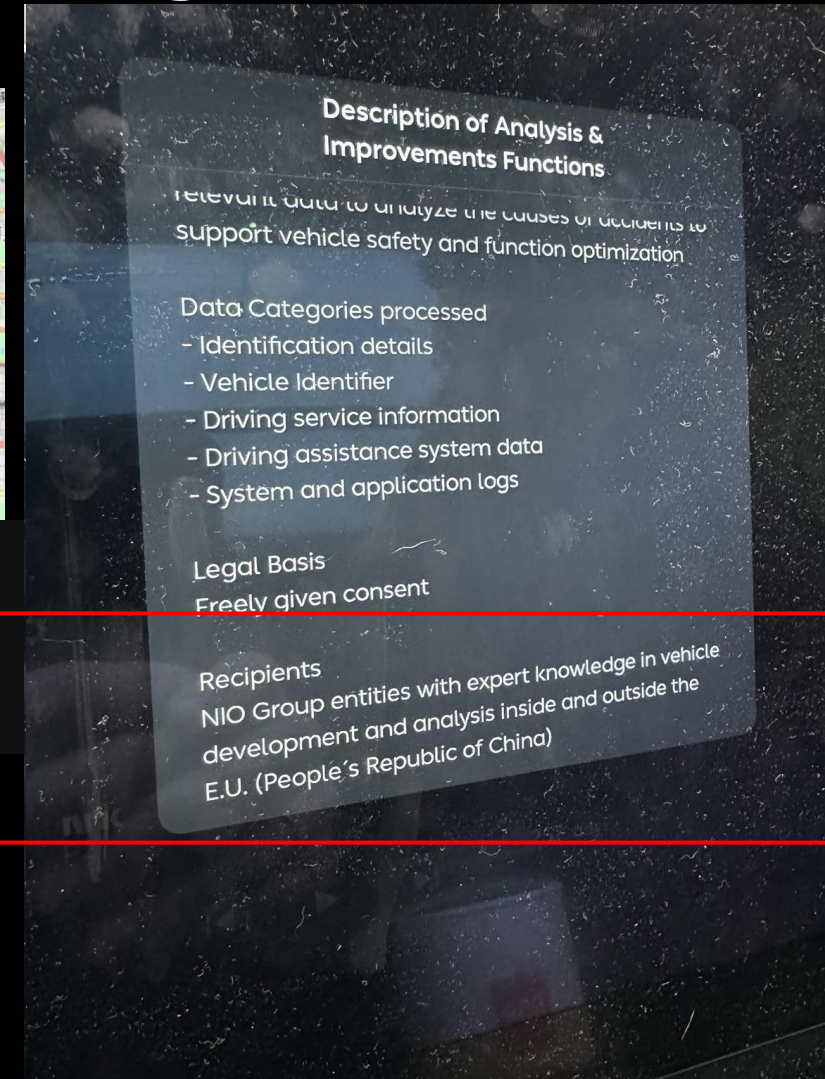


Funns: 90% av datapakkene går til og fra Kina

Eksempler på
URL'er: 163.com
China Network
Communication
Group (CNNIC),
baidu.com,
sina.com



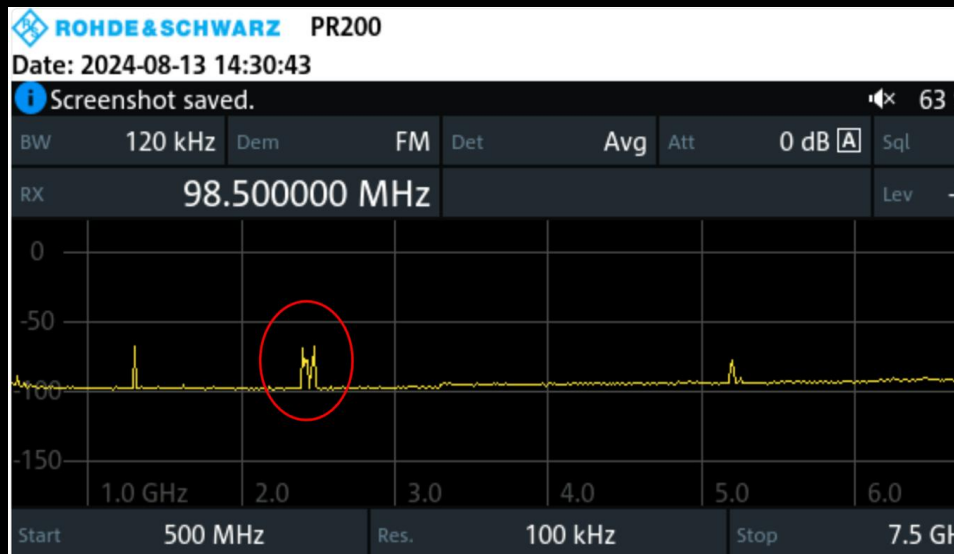
**Tor's
datapakker
sendes hit til
Beijing...**



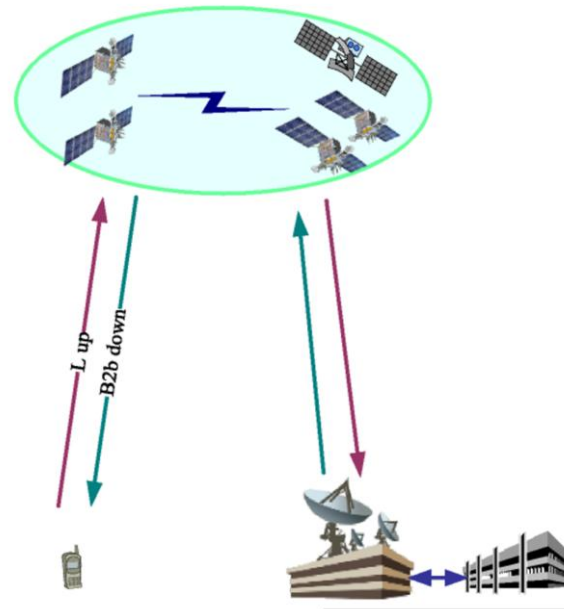
Funn: Spor etter to-veis kommunikasjon til den kinesiske GPS ekvivalenten

BeiDou (kinesiske GPS systemet) er to-veis.

1575.42MHz, 1191.79MHz, 1268.52MHz og 2492.028MHz



A Radio Determination Satellite Service (RDSS) that not only allows the user to navigate but also communicate as the very service itself is two-way between the user and the satellite(s) it is navigating via. This uplink provision can be used to allow a user to send messages to orbiting satellites as well for purely communications purposes. Interestingly, the Chinese BeiDou system is capable of RDSS which means it's a full blown two way communications system with a global reach.



NATIONAL DEFENSE UNIVERSITY PRESS
THE PREMIER PROFESSIONAL MILITARY AND ACADEMIC PUBLISHING HOUSE

Search NDU Press

HOME ABOUT ESSAY COMPETITIONS JOINT FORCE QUARTERLY PRISM OTHER PUBLICATIONS SUBMIT A MANUSCRIPT CONTACT

NEWS | April 14, 2022

BeiDou: China's GPS Challenger Takes Its Place on the World Stage

By David H. Millner, Stephen Maksim, and Marissa Huhmann
Joint Force Quarterly 105

[Download PDF](#)

Commander David H. Millner, USN, is the Senior U.S. Defense Official/Defense Attaché in Albania. Major Stephen Maksim, USSF, is Chief of the Engineering Liaison Office at the Air Force Nuclear Weapons Center. Lieutenant Commander Marissa Huhmann, USN, is currently serving as an Assistant Public Affairs Officer at U.S. Pacific Fleet.

The image shows a rocket launch from a mountainous area. The rocket is ascending, leaving a large plume of smoke and fire. The launch is taking place on a launch pad with a large structure. The background shows a mountain range and a clear sky.

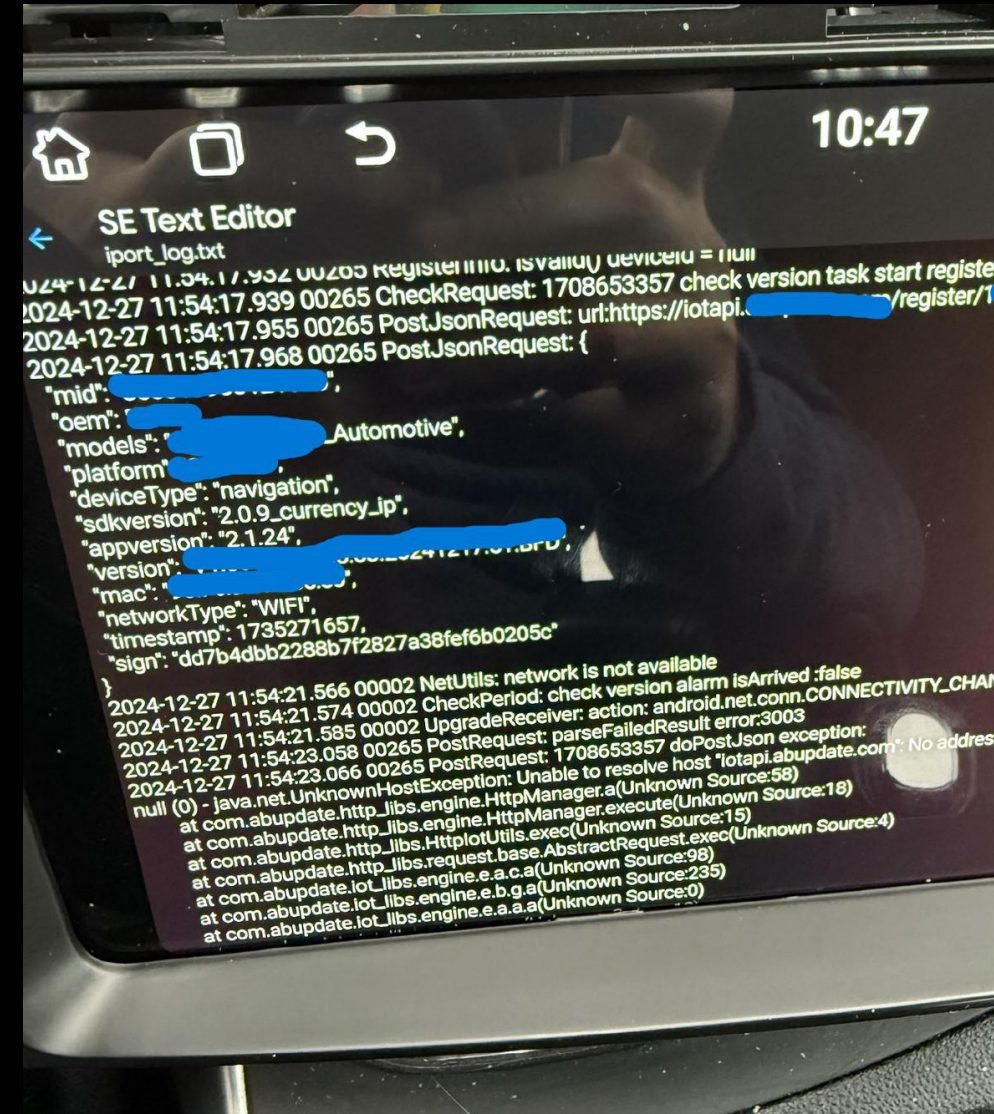
TLP:CLEAR





TLP:AMBER

Hack #1: FOTA



Hack #1: FOTA oppdateringer er sårbare

```
MySQL [iot]> SELECT table_name
<chema = "iot" ORDER BY (data_1
+-----+
| Table |
+-----+
| stats_interface_check_info_ba
| ota_pre_record
| stats_online_check_down_upgra
| stats_interface_download_info
| stats_device_area
| ota_device_version
+-----+
100 rows in set (0.79 sec)

MySQL [iot_register]> SELECT COUNT(DISTI
<) AS unique_norway FROM device_info WH
+-----+
| unique_norway |
+-----+
|          79443 |
+-----+
1 row in set (1 min 4.00 sec)

MySQL [iot_register]> []
```

```
MySQL [iot_register]> bye
-> | unique_device_count
```

```
+-----+
| 116801418 |
+-----+country_en
-> +-----+
```



Konklusjon

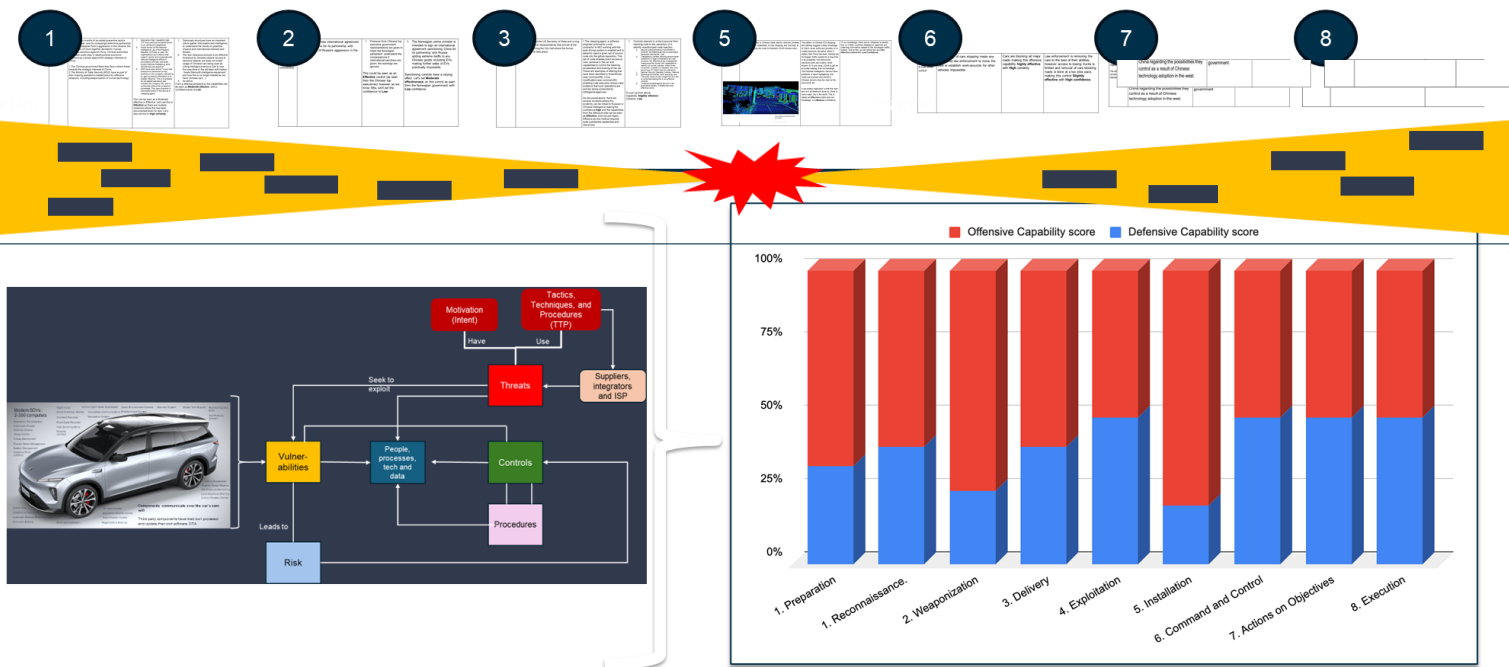
Kan bilen brukes til sabotasje?

Ja.

Og av alle

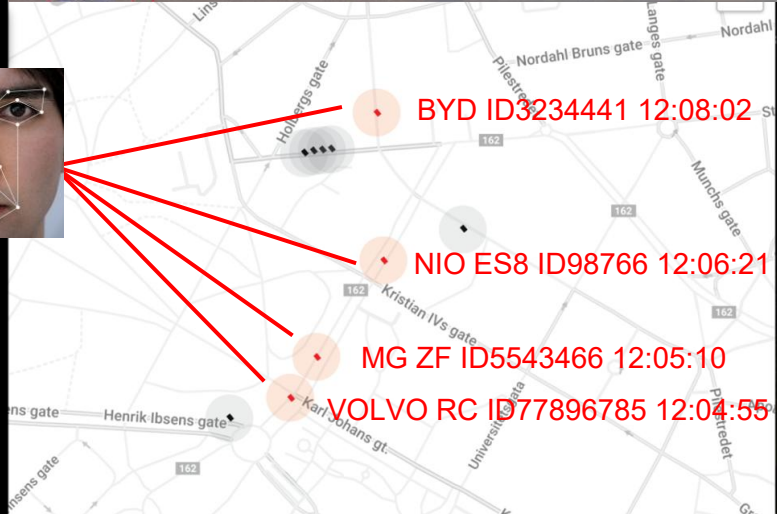
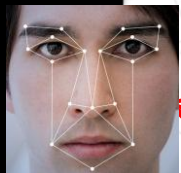
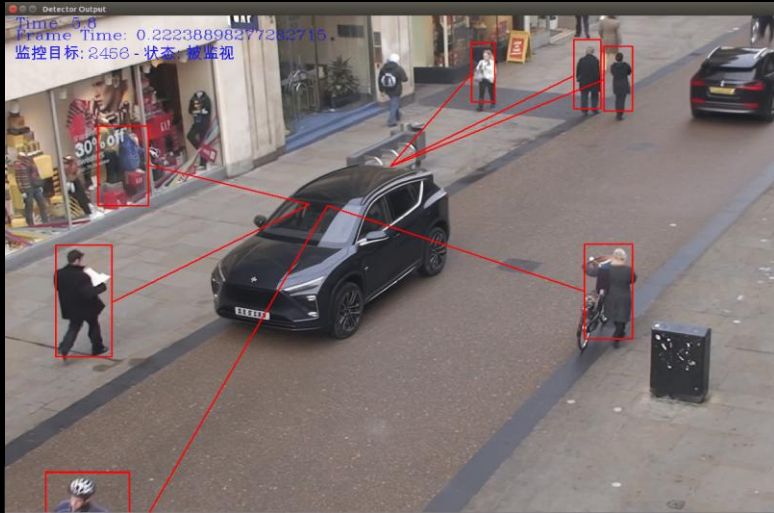
Sikkerhet er under normal standard.

Når angrepssiden vinner, strategisk risikovurdering av scenario om trafikal sabotasje



Scenariobasert tilnærming

Scenario 2 – Bil som del av overvåking



Mest sannsynlige mål:

- Kinesiske borgere: dissidenter, studenter, forskere
- Ansatte hos underleverandører i kritiske industrier og kritisk infrastruktur
- Norske POI-er (persons of interest) med innflytelse på forholdet til Kina

Kan bilen til Tor fungere som én overvåkingsplattform i et større nettverk?

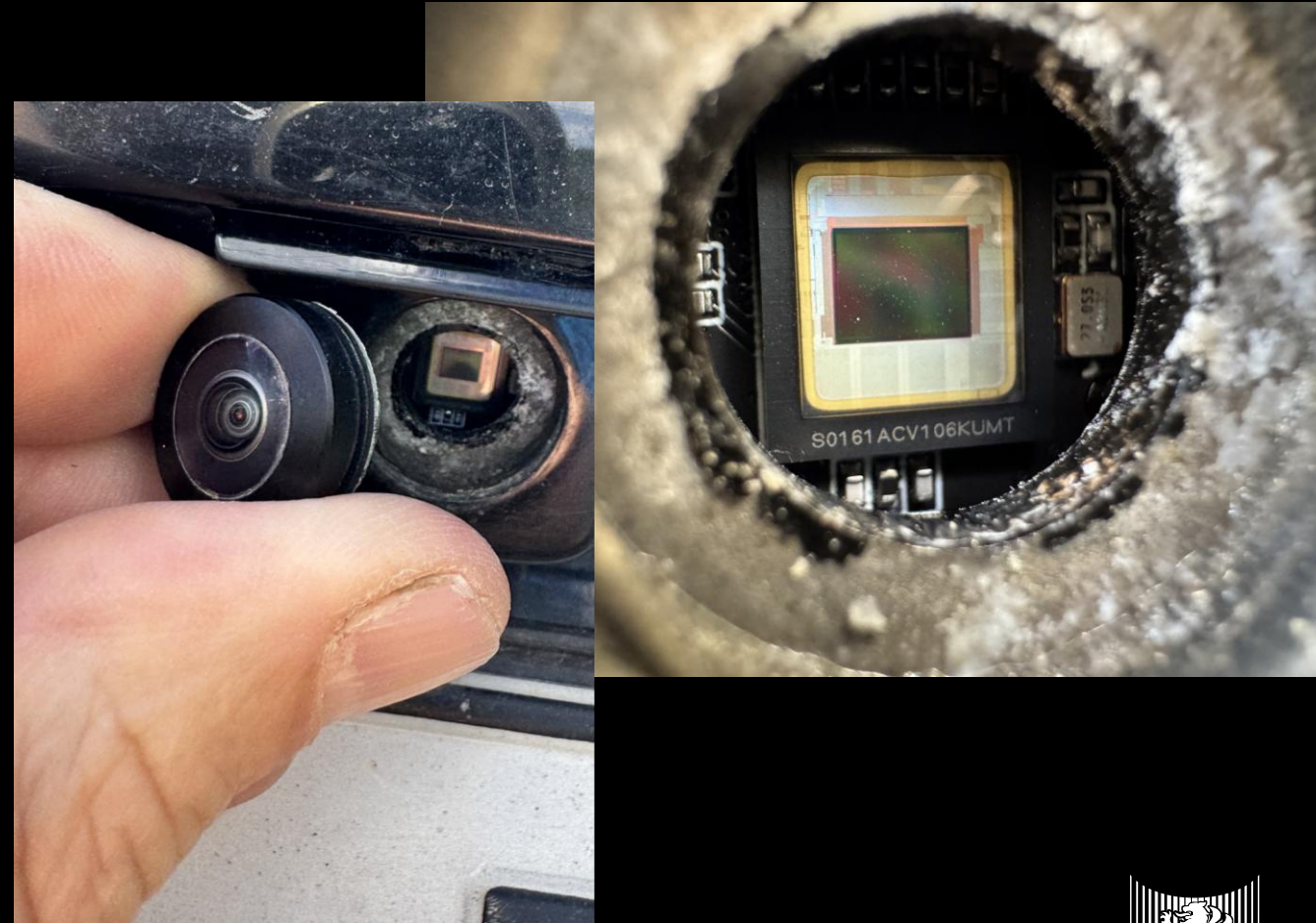


Kamera– ansikts– og skiltgjenkjenning



Camera Guidelines for Face Recognition

Match Confidence	Camera Resolution	Minimum Pixels on Face	Pixels per Meter	Pixels per Foot
High	All resolutions	80	457	137
Medium	6 MP or lower	50	286	86
	8 MP	60	343	103



TLP:CLEAR



Del 2

Teknisk
sikkerhetsvurdering
(TSA) av Busser fra VDL
og Yutong

– for Ruter



The Lion Cage Project

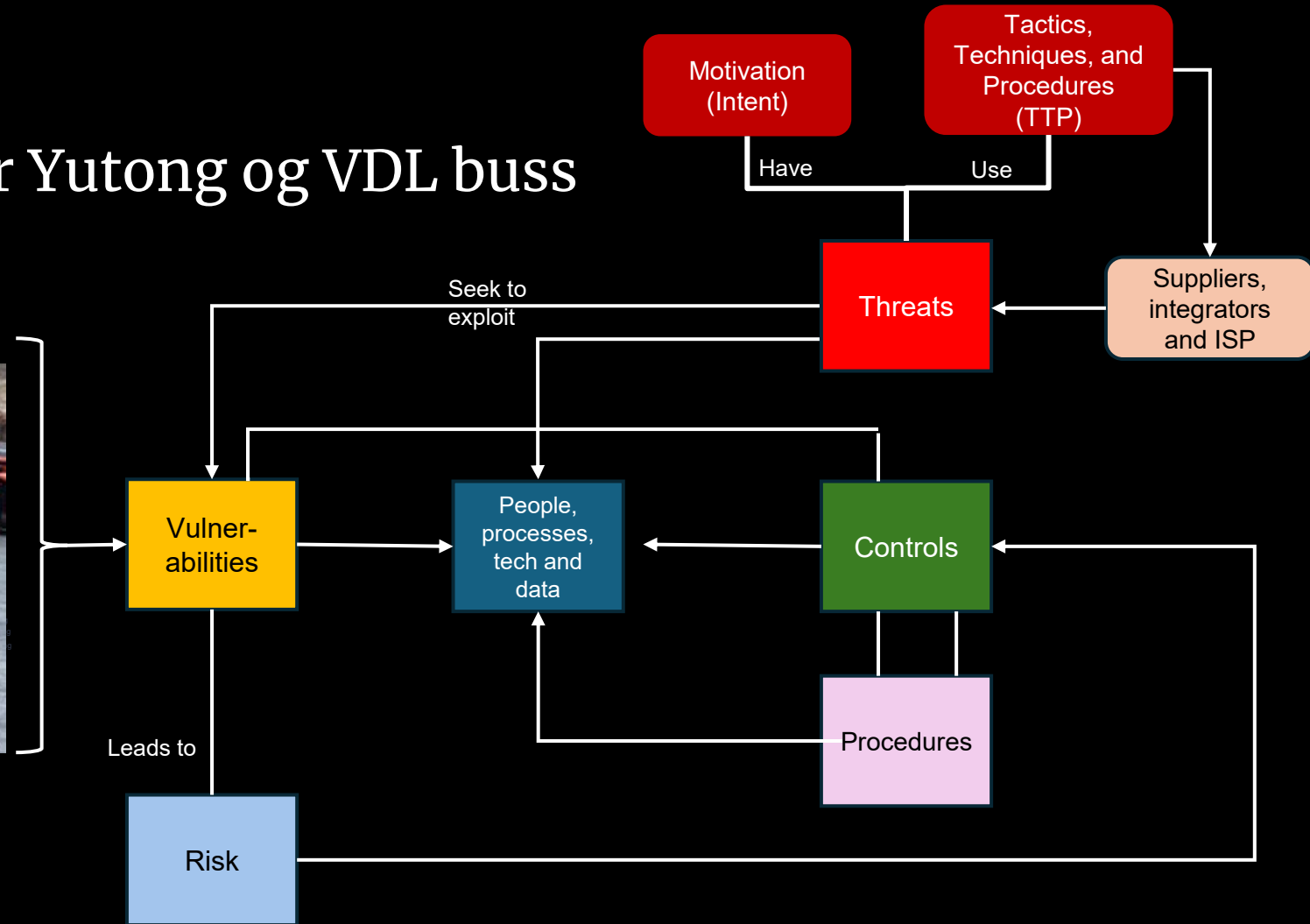
TLP:CLEAR

Del 2

Risikøkosystemet for Yutong og VDL buss

Modern SDVs:
2-300 computers
Electronic Toll Collection
Instrument Cluster
Head-Up Display
Wiper Control
Airbag Deployment
Electric Motor Management
Battery Management
Adaptive Front
Lighting

Active Yaw
Adaptive Cruise Control
Automatic Braking (Brake-by-
wire)
Anti-Lock Braking



Alle busser elektriske innen 2030 – 80 % kinesiske.

- 660 kinesiske busser i Norge (2025)
- 1200 flere på vei



Scenario 1: Kill Switch

Trafikal sabotasje, eller
trussel om sabotasje
brukt som pressmiddel

Scenario 2: Lutvann

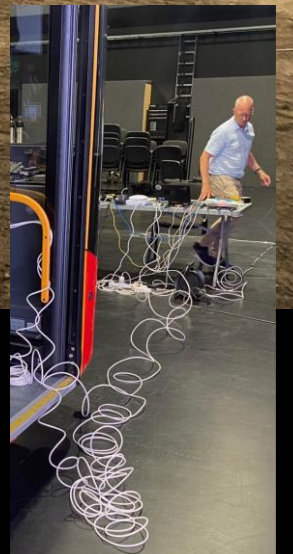
Rullende overvåking



Yutong – 2025 model og VDL – 2022 model

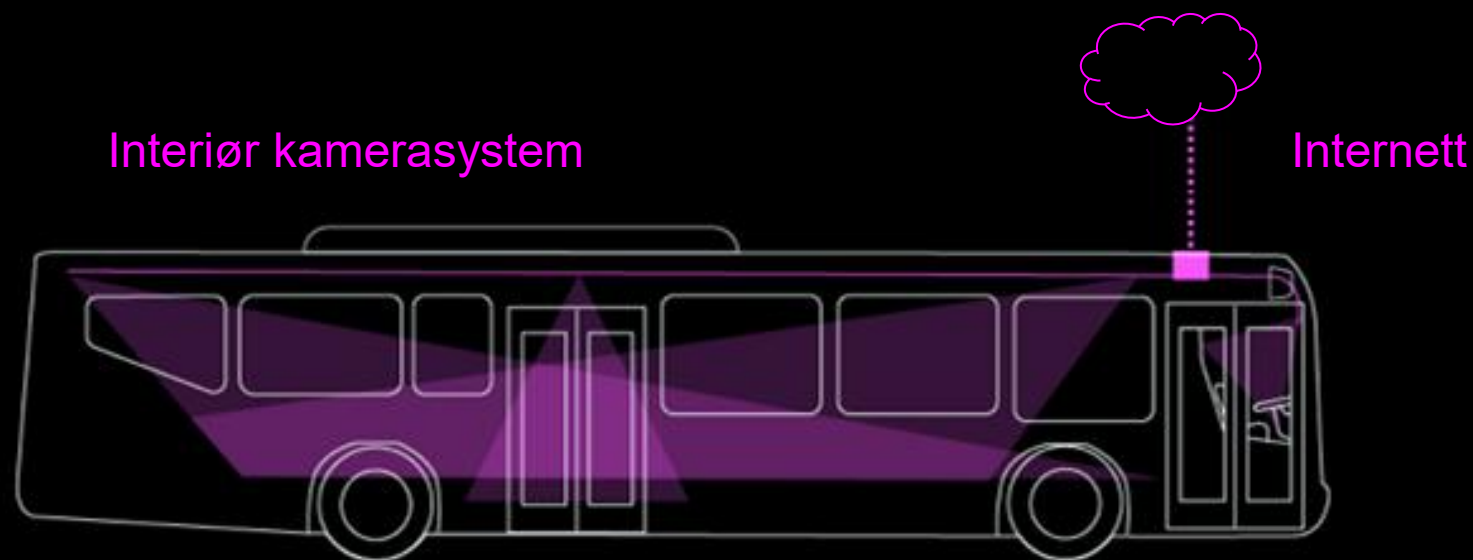


Kan VDL og/eller Yutong bussen bli brukt til Kill Switch scenarioet, eller Lutvann scenarioet?



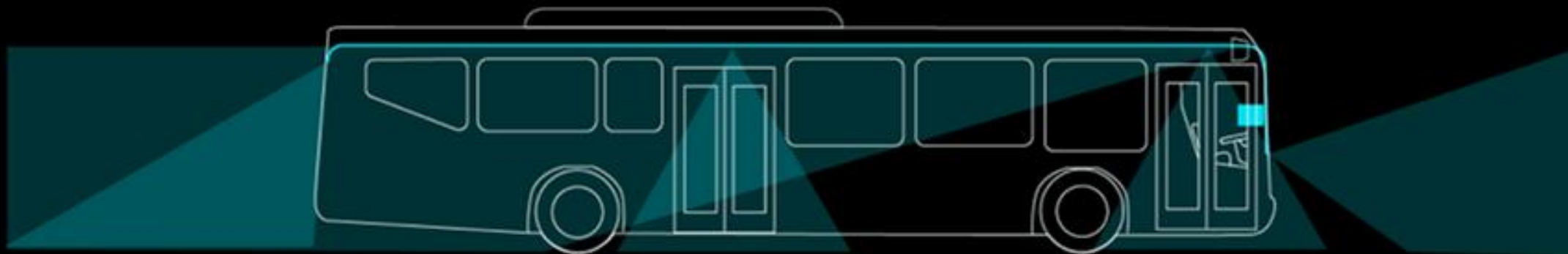
VDL – 2022 model og Yutong – 2025 model

Interiørovervåkings
funksjonaliteten er
online, til ConnectBus-
partner i Sverige.



VDL – 2022 model og Yutong – 2025 model

Eksteriør kamerasystem



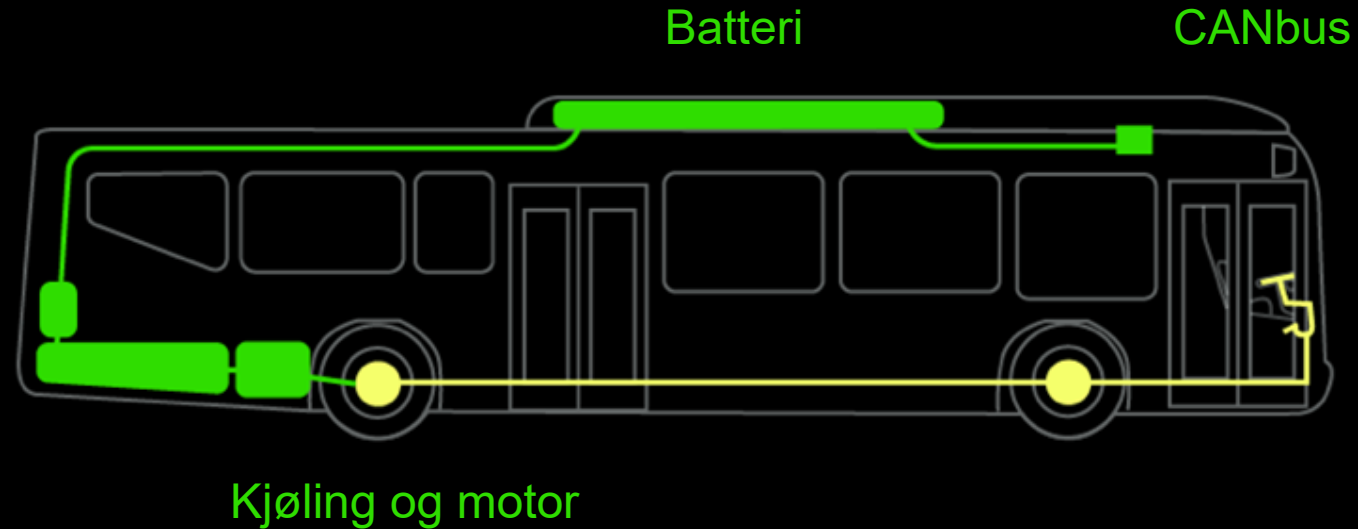
Eksteriørovervåkings-funksjonaliteten er isolert. Lutvann-scenariot, når det gjelder bilder eller video, er **ikke mulig med denne bussen.**

VDL – 2022 model

Kritisk funksjonalitet
isolert

Kill Switch ikke mulig

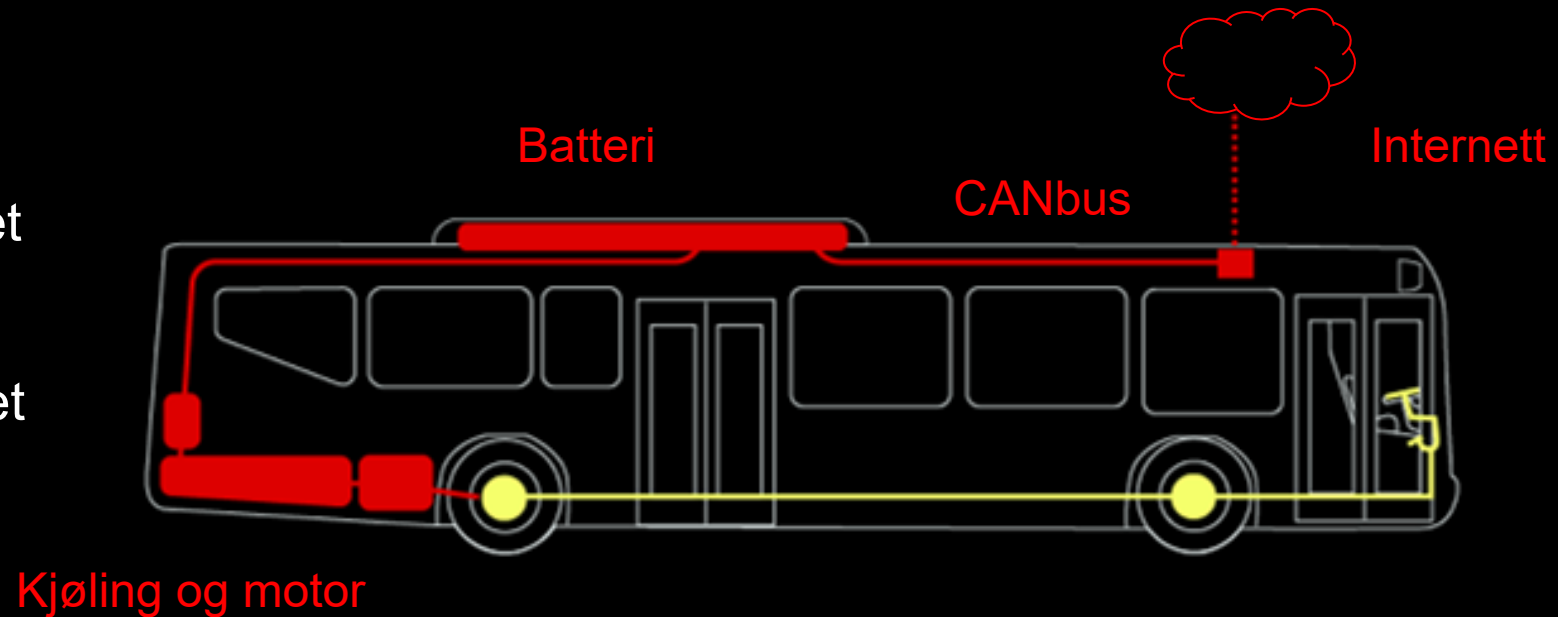
Eksteriørkamera
isolert – ingen Lutvann



Yutong – 2025 model

Kritisk funksjonalitet
er online

Kill Switch scenariet
er mulig



+ design er relativt enkelt, lite systemintegrasjoner

Yutong – 2025 model

Kritisk funksjonalitet er online.

Eksteriørkamera er isolert
Produsenten har tilgang til interne systemer. – **Kill Switch-scenarioet** er derfor mulig med denne bussen.

Eksisterende systemdesign er fortsatt enkelt, med lav grad av systemintegrasjon.



Hack #1: FOTA oppdateringer er sårbare

```
MySQL [iot]> SELECT table_name
<chema = "iot" ORDER BY (data_1
+-----+
| Table |
+-----+
| stats_interface_check_info_ba
| ota_pre_record
| stats_online_check_down_upgra
| stats_interface_download_info
| stats_device_area
| ota_device_version
+-----+

MySQL [iot_register]> SELECT COUNT(DISTI
<) AS unique_norway FROM device_info WH
+-----+
| unique_norway |
+-----+
|          79443 |
+-----+
1 row in set (1 min 4.00 sec)

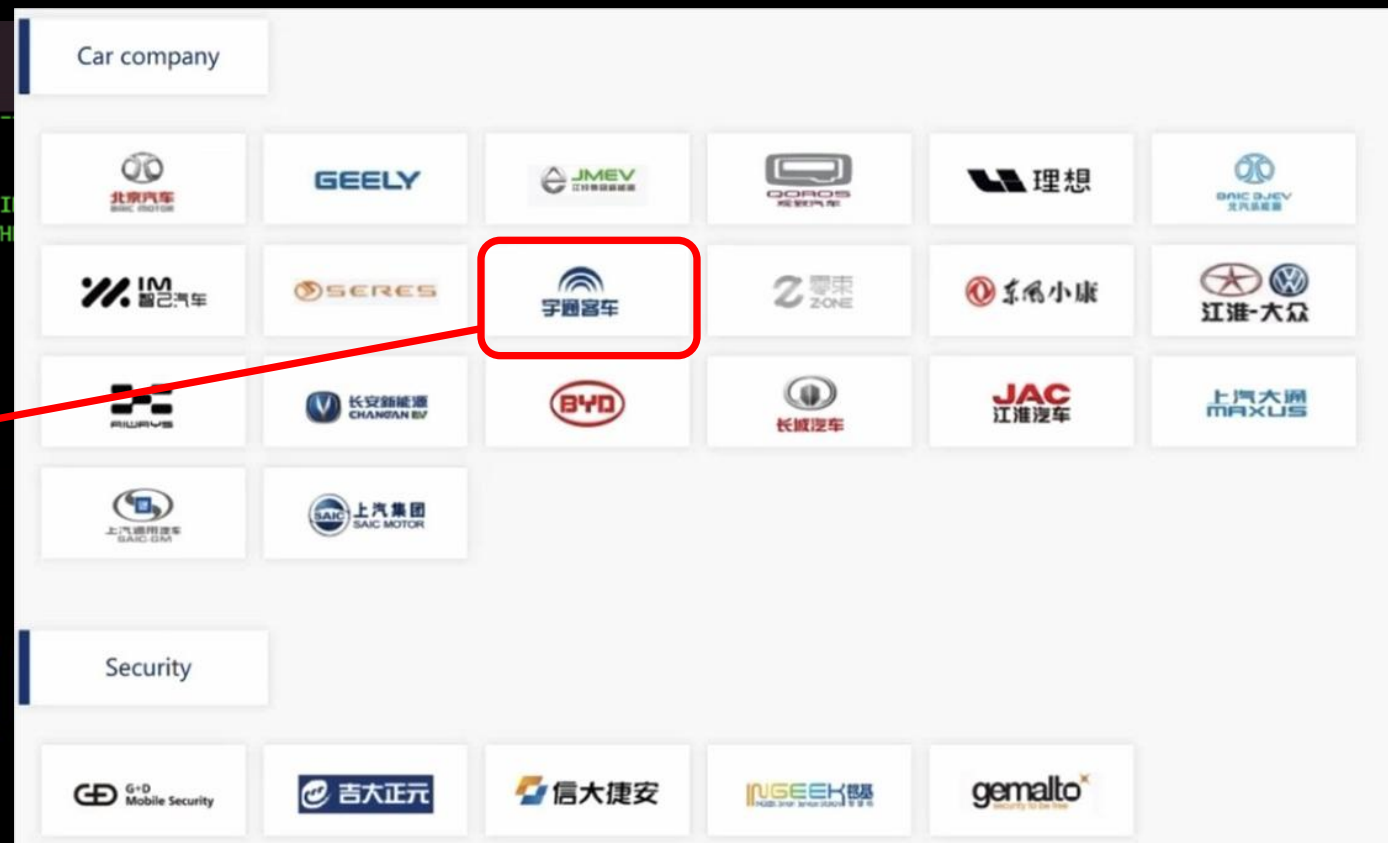
MySQL [iot_register]> []
```

```
MySQL [iot_register]> bye
-> | unique_device_count
```

```
+-----+
| 116801418 |
+-----+country_en
-> +-----+
```



Hack #1: FOTA oppdateringer er sårbare



More about the BYD's "God's Eye" driving assistance system

BYD officials revealed that the "God's Eye" ADAS system has three intelligent driving classifications. The entry-level system is called "God's Eye C". It relies on a three-camera cluster sitting behind the windshield. As the entry-level tier ADAS system, the "God's Eye C" will be adopted by cars under the BYD brand. This perception system will be powered by the DiPilot 100 system with a peak computing power of 100 TOPS.

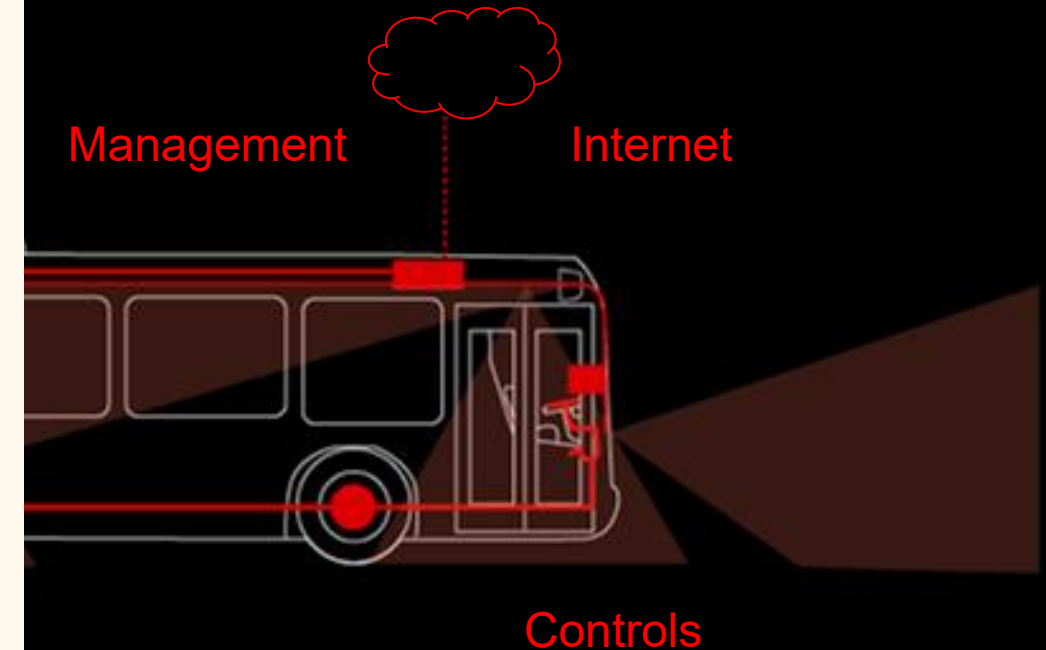
BYD next gen:

- 12 cameras
- 3 front-view
- 5 panorama
- 4 surround view
- 5 mm wave radar
- 12 ultrasonic radar



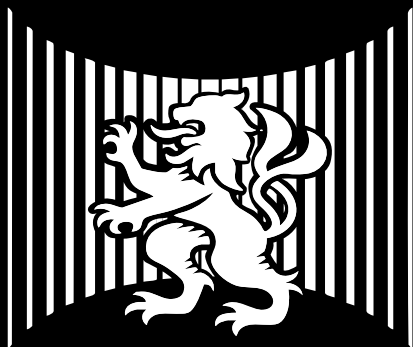
Other hardware elements of the "God's Eye C" include 12 cameras, 5 mm-wave radars, and 12 ultrasonic radars. Those 12 cameras consist of 3 front-view cameras, 5 panoramic cameras, and 4 surround-view cameras. Five mm-wave radars provide 360-degree non-dead angle perception, the front radar has a detection distance of 300 meters. The accuracy of the 12 ultrasonic radar sensors is 1 cm, and the parking accuracy is 2 cm.

usser = droner



systemer, inkludert
ør legges i smarte





Tor Indstøy – VP of Risk Management and Threat Intelligence at Telenor Group
tor.indstoy@telenor.com

Arild Tjomsland – Special Advisor TTO at the University of Southeast Norway
arild.tjomsland@usn.no

All technical details at [Lion Cage on LinkedIn](#)