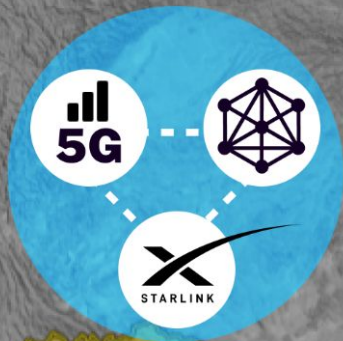






The single innovation that will reshape the modern battlefield in our lifetime — **the portable smartphone**



We need a next gen PACE Plan...especially in the in an Anti-Access Area Denial (A2D2) fight

South Korea

Japan

Taiwan

Philippines

Guam

**The ACE fight is on in
INDOPACOM.**



**Networks are being
savagely attacked**



You hear a BOOM...



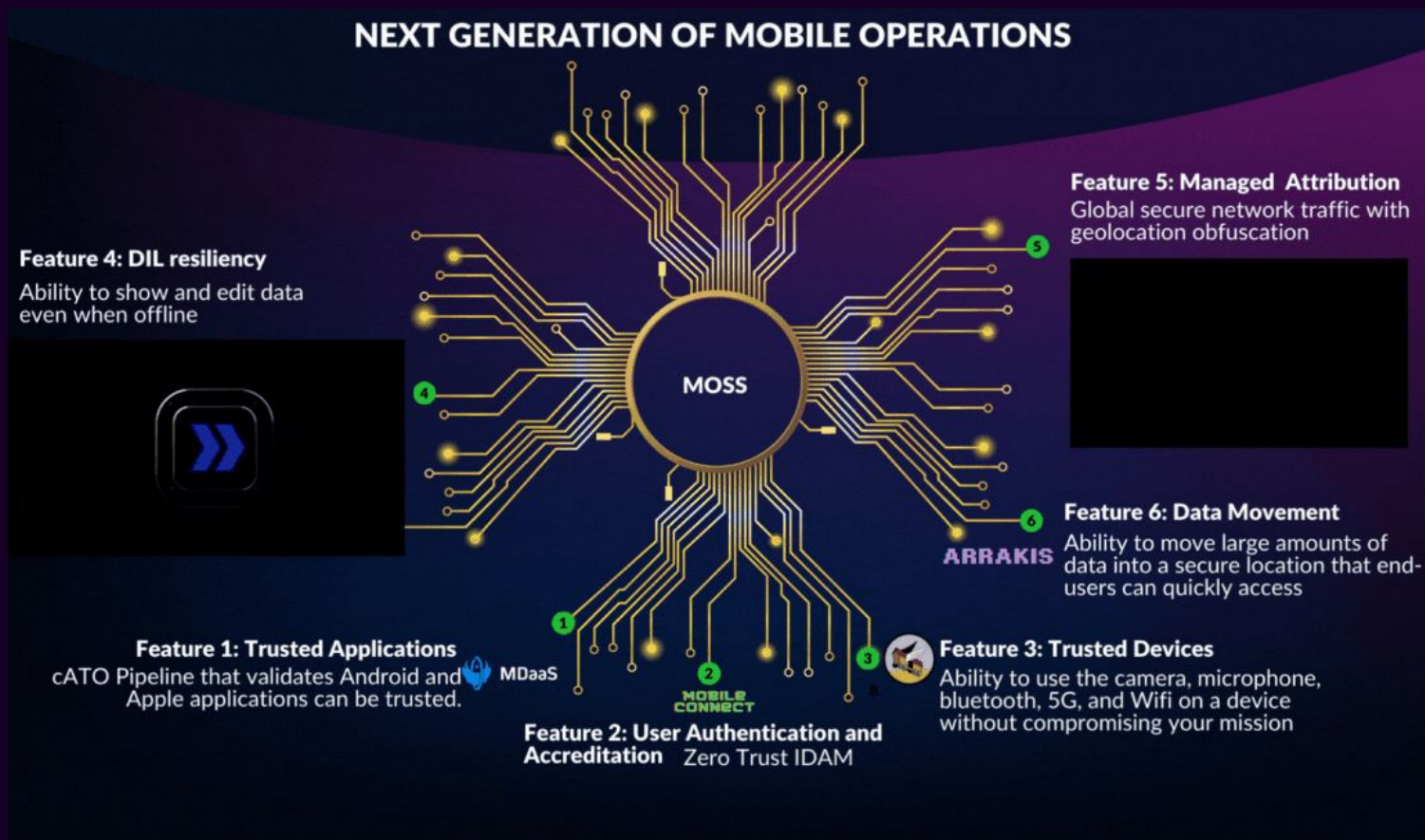
What do we do?!



**No C2 = Chaos in the
MOC**



Luckily
we
have
MOSS



BDA Team



Report up!



**Airfield MX and EOD
has arrived!**



**Airfield MX and EOD
has arrived!**

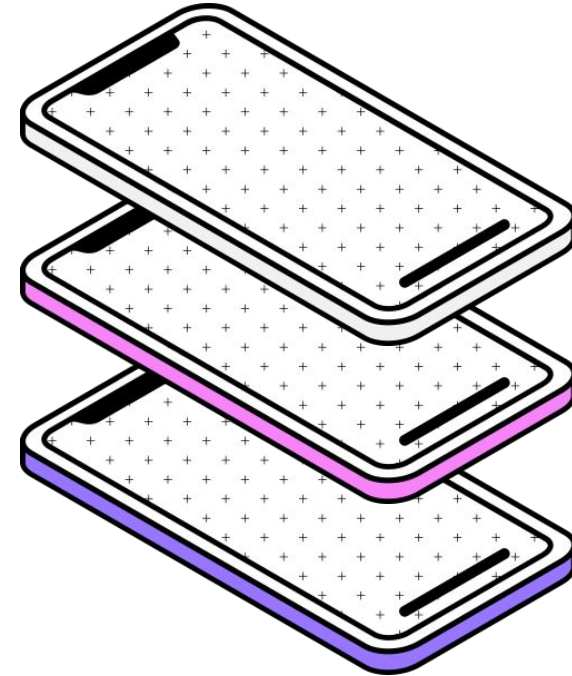


**Long haul connection
is re-established.**



Supercomputer in your pocket

Portability	Multiple connectivity options	Offline Capabilities (Mesh & mobile native apps)
More computing power than standard PC*	Built-in camera and sensors	Biometric Authentication
App Stores	Quick Boot-up times	Cloud Integration



+ Familiarity and Habituation

Why MOSS?

The future fight isn't in a 5 hour operational window. It's continuous, unfair, and unreliable.

Our capabilities need to achieve a state of adaptability that we've never seen before.

MOSS takes an already extremely compelling and easy-to-use Platform (mobile devices) and makes it DoD relevant.

Why MOSS matters?

CBS NEWS

NEWS

SHOWS

LIVE

LOCAL

Q

Login

POLITICS

CIA Director William Burns: "I wouldn't underestimate" Xi's ambitions for Taiwan

BY OLIVIA GAZIS

FEBRUARY 3, 2023 / 7:38 PM / CBS NEWS



Intelligence shows Chinese president Xi Jinping has instructed his co- a successful invasion" of Taiwan, CIA Director William Burns said. It's not clear whether Xi had actually decided to use military force.

Taiwan foreign minister warns of conflict with China in 2027

Comments indicate extent to which Taiwan is trying to bolster western support before possible invasion



Joseph Wu

Reuters/Reuters

Taiwan's foreign minister has said he is preparing for the possibility of a conflict with China in 2027.

CIA director: China readying for Taiwan invasion by 2027

Xi wants China's military ready to invade within four years, CIA Director William Burns said.

Alex Willemyns for RFA

2023.02.03

Washington

Military > Pop Mech Pro Military

The U.S. Military 'Failed Miserably' in a Fake Battle Over Taiwan

The Pentagon has been fighting wars the same way for decades. What happens if someone is taking notes?



BY KYLE MIZOKAMI

PUBLISHED: AUG 2, 2021

SAVE ARTICLE



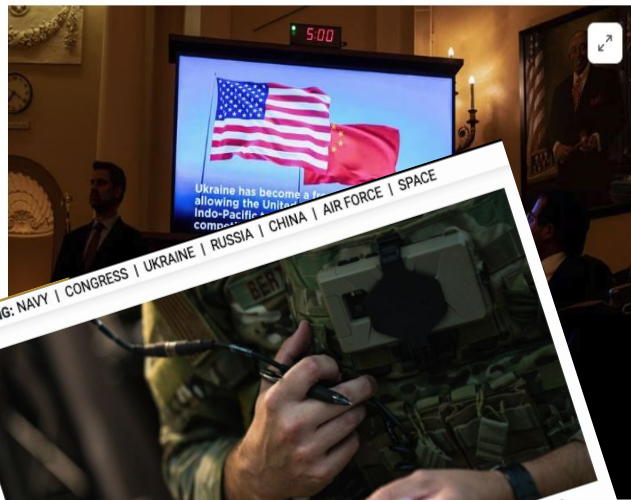
US war game on Taiwan shows need for 'decisive action' to boost arms

By Michael Martina

April 20, 2023 11:48 AM EDT · Updated 5 months ago

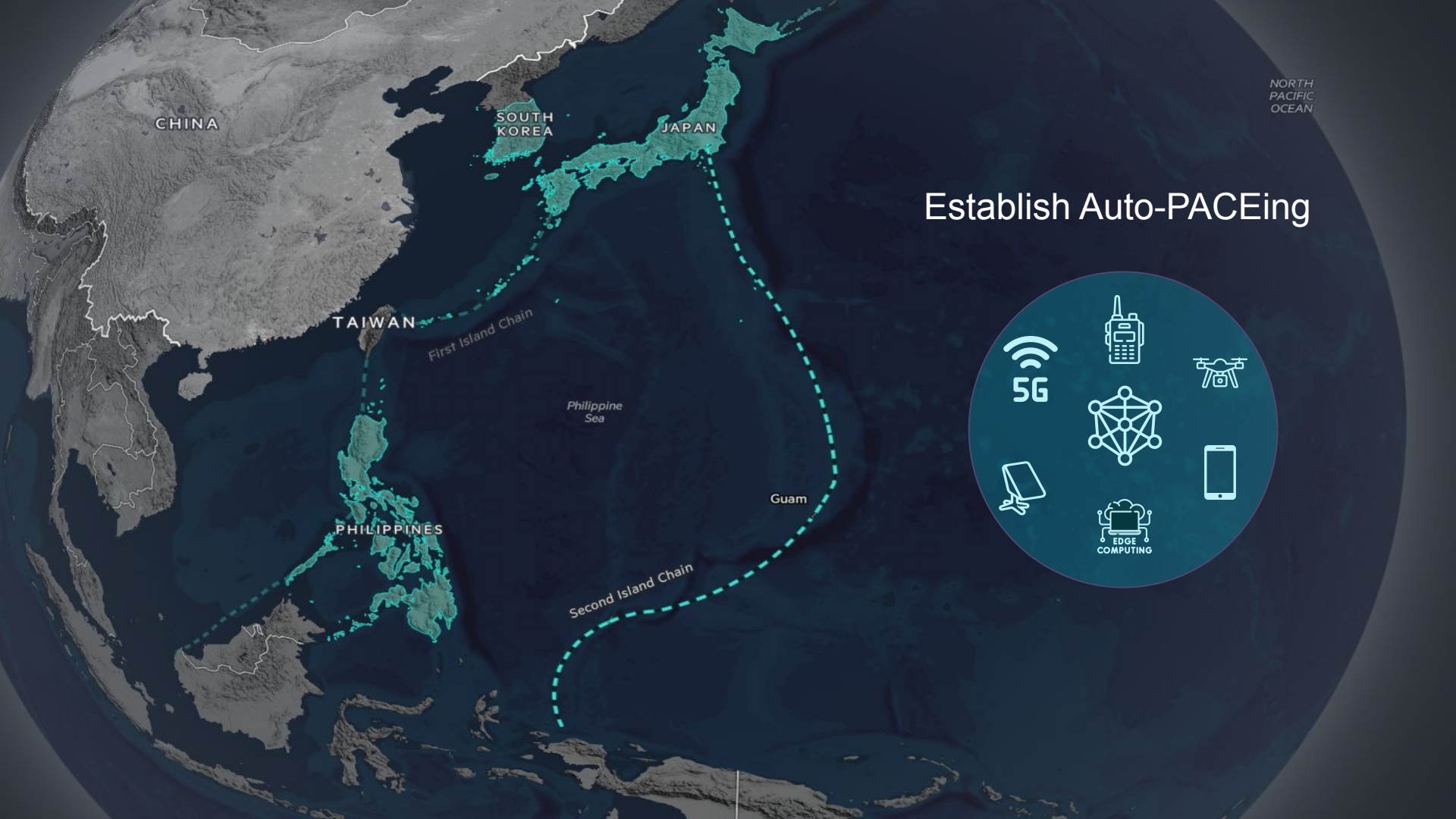


Aa



'It Failed Miserably': After Wargaming Loss, Joint Chiefs Are Overhauling How the US Military Will Fight

In a fake battle for Taiwan, U.S. forces lost network access almost immediately. Hyten has issued four directives to help change that.



NORTH
PACIFIC
OCEAN

Establish Auto-PACEing



WORLD >

Unauthorized use of cellphones by Russian soldiers led to Ukrainian strike that killed 89 troops, military says

JANUARY 4, 2023 / 9:36 AM EST / CBS/AP



CBS MORNINGS

UKRAINE STRIKE KILLS DOZENS OF RUSSIAN TROOPS

How does MOSS enable warfighters?

Demographics: Up to 35,000 users

- US Army -Special Forces, Rangers
- USMC -Recon, Radier
- USN -SEALs, SARC
- USAF -Combat Control, PJ, TACP

Special Operators



Mobile Needs

Special Operators

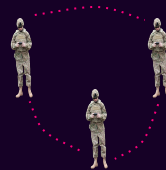
Access to secure apps & devices: access to trusted (CUI, Classified) apps onto the trusted device



Mobile Needs

Special Operators

Access to secure apps & devices: access to trusted (CUI, Classified) apps onto the trusted device

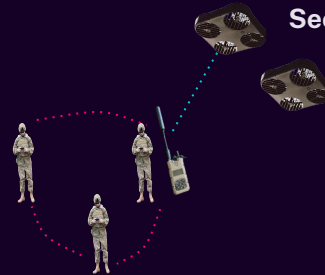


Disconnected Ops: ability to show, edit, and share data even when offline

Mobile Needs

Special Operators

Access to secure apps & devices: access to trusted (CUI, Classified) apps onto the trusted device

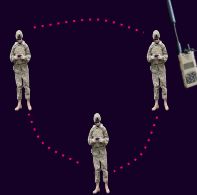


Secure Military drone connectivity: managed attribution for devices on network

Disconnected Ops: ability to show, edit, and share data even when offline

Mobile Needs

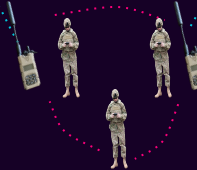
Long range data sync: troops can sync long distance within local mesh



Secure Military drone connectivity: managed attribution for devices on network



Disconnected Ops: ability to show, edit, and share data even when offline



Access to secure apps & devices: access to trusted (CUI, Classified) apps onto the trusted device



Special Operators

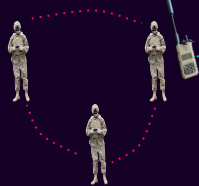


Mobile Needs

Data movement: ability to move large amounts off a mobile device quickly



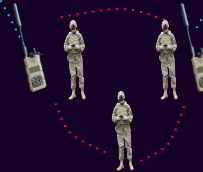
Long range data sync: troops can sync long distance within local mesh



Secure Military drone connectivity: managed attribution for devices on network



Disconnected Ops: ability to show, edit, and share data even when offline



Access to secure apps & devices: access to trusted (CUI, Classified) apps onto the trusted device



Special Operators



Mobile Needs

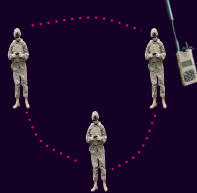
Global accessibility: ability to leverage resilient transit across globally diverse paths



Data movement: ability to move large amounts off a mobile device quickly



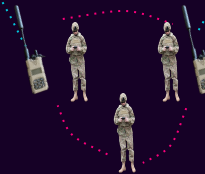
Long range data sync: troops can sync long distance within local mesh



Secure Military drone connectivity: managed attribution for devices on network



Disconnected Ops: ability to show, edit, and share data even when offline



Access to secure apps & devices: access to trusted (CUI, Classified) apps onto the trusted device



Special Operators



MOSS eliminates mobile fears.

MOSS: MITIGATING RISKS AND FEARS THAT PREVENT MOBILE OPERATIONS

Location Tracking

Unprotected Data
Transfer

Insufficient Cryptography

Audio Capture

Video Capture

Improper Credential
Usage

Reverse Engineering

Unapproved App Usage

App Supply Chain
Security

Code quality

Large Scale Data
Movement

Insecure Authentication

Insecure Communication

Disconnected, Intermittent,
and Low Bandwidth Env

Insecure Devices

MOSS MITIGATION APPROACHES



MDaaS

MOSS: NEXT GENERATION OF MOBILE OPERATIONS

6. Device Management

5. User Authentication and Accreditation

4. Managed Attribution: Zero Trust Networks

3. Disconnected, Intermittent, and Low Bandwidth Env

2. Self Service Data Lake

1. Custom and pre-vetted Mobile apps



BESPIN



MDaaS

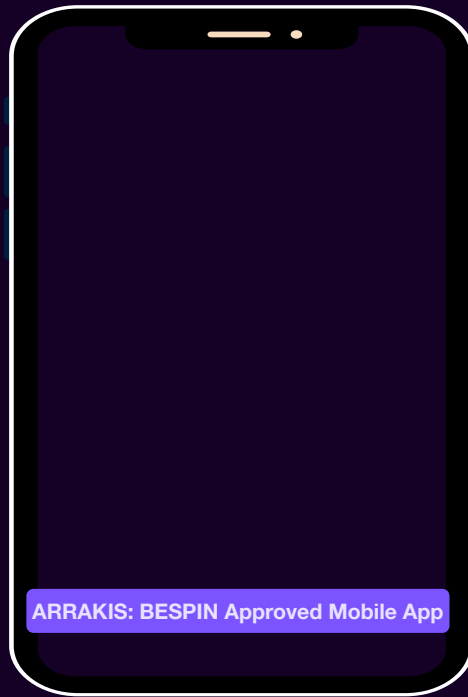
MOSS: MITIGATING RISKS AND FEARS THAT PREVENT MOBILE OPERATIONS

Location Tracking	Unprotected Data Transfer	Insufficient Cryptography
Audio Capture	Video Capture	Improper Credential Usage
Reverse Engineering	Unapproved App Usage	App Supply Chain Security
Code quality	Large scale data Movement	Insecure Authentication
Insecure Communication	Disconnected, Intermittent, and Low Bandwidth Env	Insecure Devices

MOSS MITIGATION APPROACHES



MDaaS



ARRAKIS: BESPIN Approved Mobile App

Self Service Data Lake

ARRAKIS: Self Service Data Lake

I have data where should I put it?
I need data where should I go?

Data Set Tagging
Time Stamp
Metadata Rules



Mission Data



AWS



RISKS AND FEARS THAT PREVENT MOBILE OPERATIONS

Location Tracking	Unprotected Data Transfer	Insufficient Cryptography
Audio Capture	Video Capture	Improper credential usage
Reverse Engineering	Unapproved App Usage	App Supply Chain Security
Code quality	Large Scale Data Movement	Insecure Authentication
Insecure Communication	Disconnected, Intermittent, and Low Bandwidth Env	Insecure Devices

MOSS MITIGATION APPROACHES



MDaaS

ARRAKIS



BESPIN

Disconnected, Intermittent, and Low Bandwidth Env

DITTO: Software Development Kit

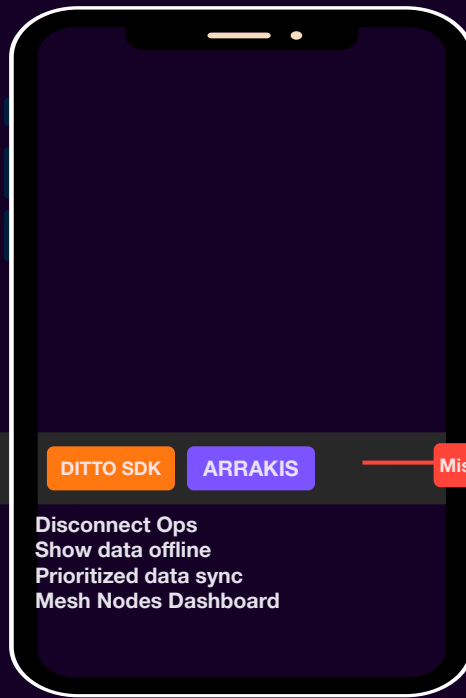
TLS Encrypted Mesh Network
Apps with Ditto can sync w/o internet
Share, show, and edit data when offline

Self Service Data Lake

ARRAKIS: Self Service Data Lake

I have data where should I put it?
I have data where should I go?

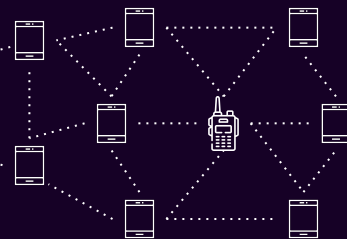
Data Set Tagging
Time Stamp
Metadata Rules



Mission Data

DITTO Small Peer

Mission Data



DITTO Big Peer

AARKIS

AARKIS

AWS

BESPIN
Mobile App
Dev
Platform

RISKS AND FEARS THAT PREVENT MOBILE OPERATIONS

Location Tracking	Unprotected Data Transfer	Insufficient Cryptography
Audio Capture	Video Capture	Improper credential usage
Reverse Engineering	Unapproved App Usage	App Supply Chain Security
Code quality	Large Scale Data Movement	Insecure Authentication
Insecure Communication	Disconnected, Intermittent, and Low Bandwidth Env	Insecure Devices

MOSS MITIGATION APPROACHES



MDaaS

ARRAKIS

» ditto



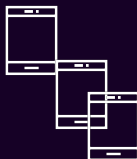
BESPIN

Managed Attribution: Zero Trust Networks

STUN: Secure Transit over Unclass Networks

Geolocation Obfuscation
End-to-End IP Transec
Network Path Dissemination
User defined and non-attribution
globally positioned relay nodes

STUN Enabled
TRANSEC as a service



Disconnected, Intermittent, and Low Bandwidth Env

DITTO: Software Development Kit

TLS Encrypted Mesh Network
Apps with Ditto can sync w/o internet
Share, show, and edit data when offline

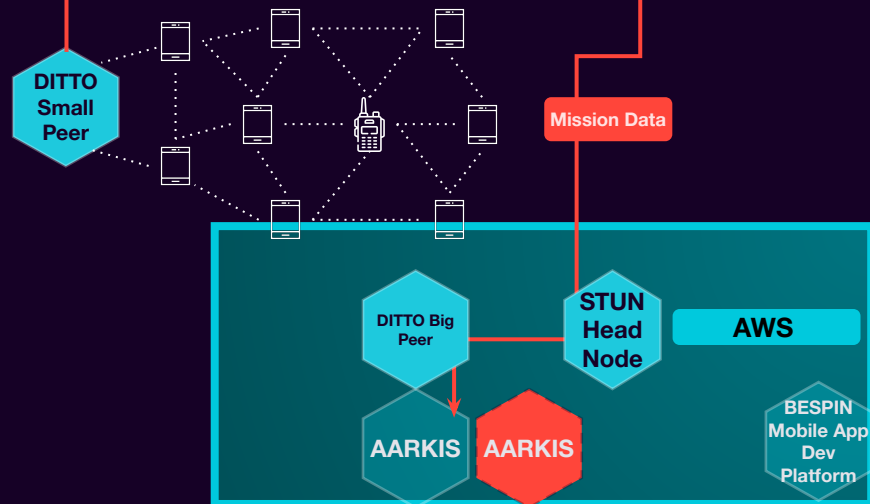
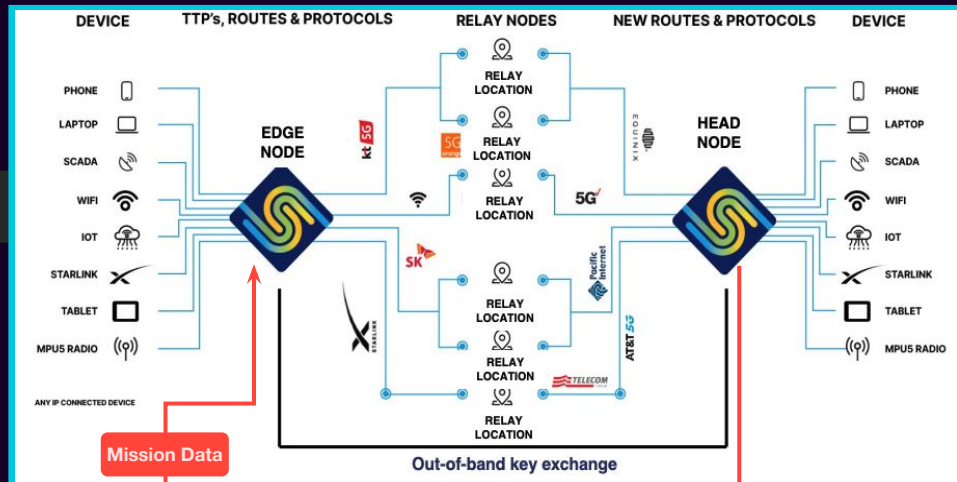
Self Service Data Lake

ARRAKIS: Self Service Data Lake

I have data where should I put it?
I have data where should I go?

Data Set Tagging
Time Stamp
Metadata Rules

User defined and non-attribution, globally positioned relay nodes



Managed Attribution: Zero Trust Networks

STUN: Secure Transit over Unclass Networks

- Geolocation Obfuscation
- End-to-End IP Transec
- Network Path Dissemination
- Globally positioned relay nodes

Disconnected, Intermittent, and Low Bandwidth Env

DITTO: Software Development Kit

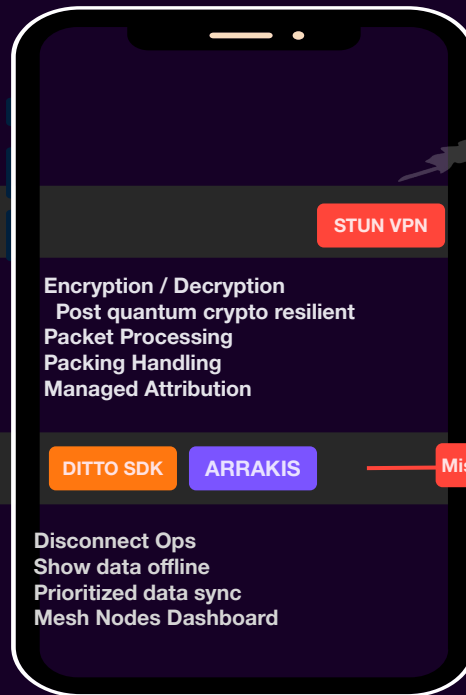
- TLS Encrypted Mesh Network
- Apps with Ditto can sync w/o internet
- Share, show, and edit data when offline

Self Service Data Lake

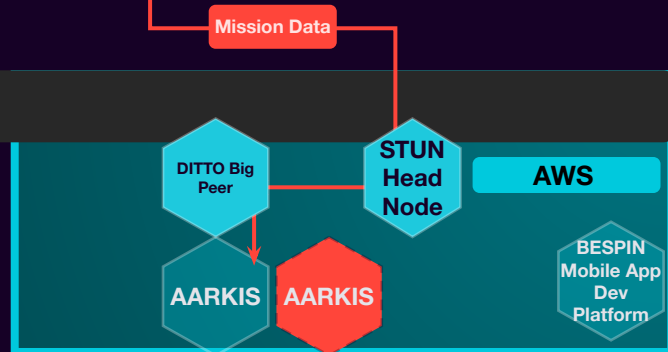
ARRAKIS: Self Service Data Lake

- I have data where should I put it?
- I have data where should I go?

- Data Set Tagging
- Time Stamp
- Metadata Rules



USER DEFINED GLOBAL RELAY NODES



RISKS AND FEARS THAT PREVENT MOBILE OPERATIONS

Location Tracking	Unprotected Data Transfer	Insufficient Cryptography
Audio Capture	Video Capture	Improper credential usage
Reverse Engineering	Unapproved App Usage	App Supply Chain Security
Code quality	Large Scale Data Movement	Insecure Authentication
Insecure Communication	Disconnected, Intermittent, and Low Bandwidth Env	Insecure Devices

MOSS MITIGATION APPROACHES



MDaaS

ARRAKIS

» ditto



BESPIN

User Authentication and Accreditation

Managed Attribution: Zero Trust Networks

STUN: Secure Transit over Unclass Networks

Geolocation Obfuscation
End-to-End IP Transec
Network Path Dissemination
Globally positioned relay nodes

Disconnected, Intermittent, and Low Bandwidth Env

DITTO: Software Development Kit

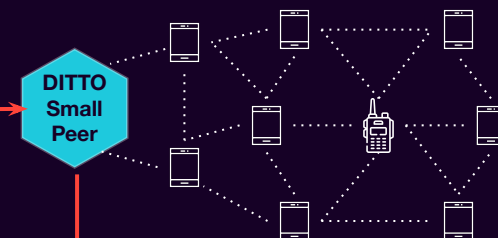
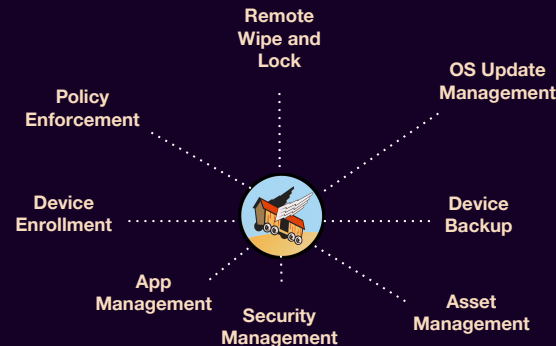
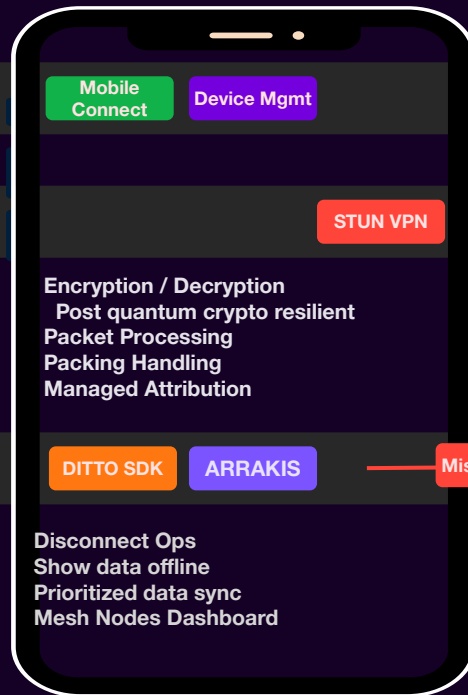
TLS Encrypted Mesh Network
Apps with Ditto can sync w/o internet
Share, show, and edit data when offline

Self Service Data Lake

ARRAKIS: Self Service Data Lake

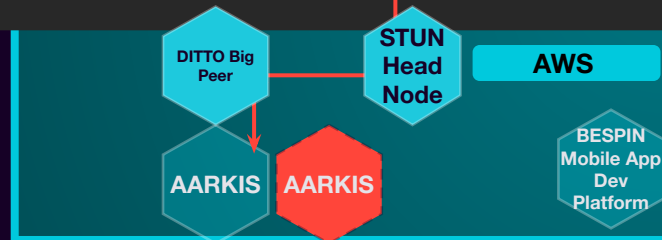
I have data where should I put it?
I have data where should I go?

Data Set Tagging
Time Stamp
Metadata Rules



Mission Data

Mission Data



RISKS AND FEARS THAT PREVENT MOBILE OPERATIONS

Location Tracking	Unprotected Data Transfer	Insufficient Cryptography
Audio Capture	Video Capture	Improper credential usage
Reverse Engineering	Unapproved App Usage	App Supply Chain Security
Code quality	Insecure Data Storage	Insecure Authentication
Insecure Communication	Disconnected, Intermittent, and Low Bandwidth Env	Insecure Devices

MOSS MITIGATION APPROACHES



MDaaS

ARRAKIS

>>ditto



MobileConnect



BESPIN