MILCOM 2017

MILITARY COMMUNICATIONS AND INNOVATION - PRIORITIES FOR THE MODERN WARFIGHT

Data-Centric Battlefield

What is IoBT?

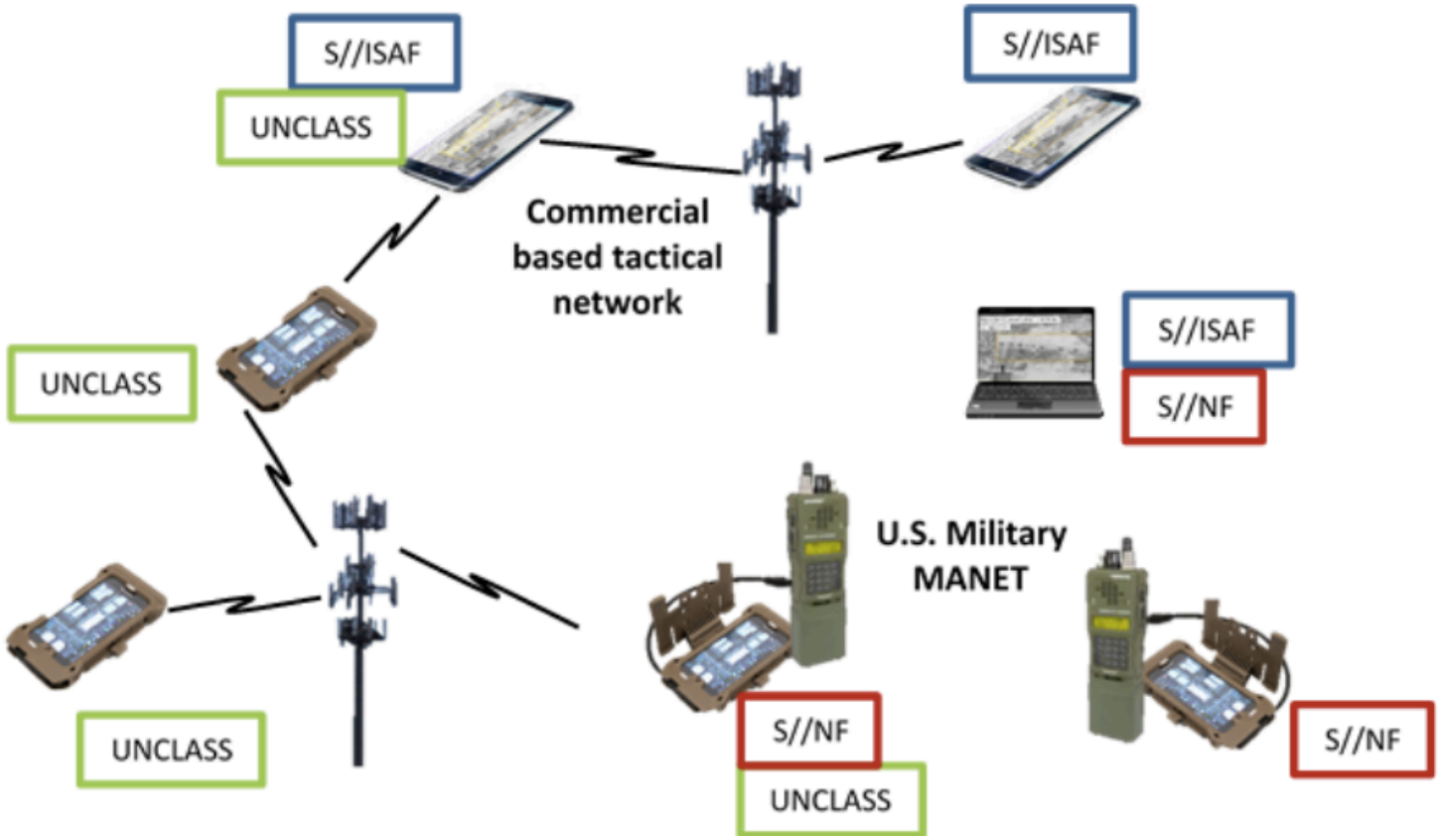
- ***An IoBT is…*** a set of interdependent and interconnected entities or "things"
  - → Sensors
  - → Actuators
  - → Devices (computers, weapons, vehicles, robots, human-wearables…)
  - → Infrastructure (networks, storage, processing)
  - → Analytics (on-node, in-network, centralized)
  - → Information sources & Open Source Intelligence
  - → Humans

- ***That are…*** Dynamically composed to meet multiple missions, tasks, or goals
- **And…** Adapt to capture/process data, predict behaviors/activities, and effectuate the physical environment
- **And are likely to…** operate autonomously and autonomically, i.e. properties include Self-Star characteristics (Self* = *SELF* organizing, configuring, adapting, maintaining, protecting)
- **Necessarily…** Interacting with humans, environment, networks
- **In order…** To provide intelligent command and control and battlefield services

Objective: Develop a fundamental understanding of dynamically composable, adaptive, goal-driven IoBTs, enabling distributed analytics for intelligent C^2 and battlefield services

NDN is making its way to the tactical edge

- Secure Handhelds on Assured Resilient networks at the tactical Edge (SHARE) DARPA program

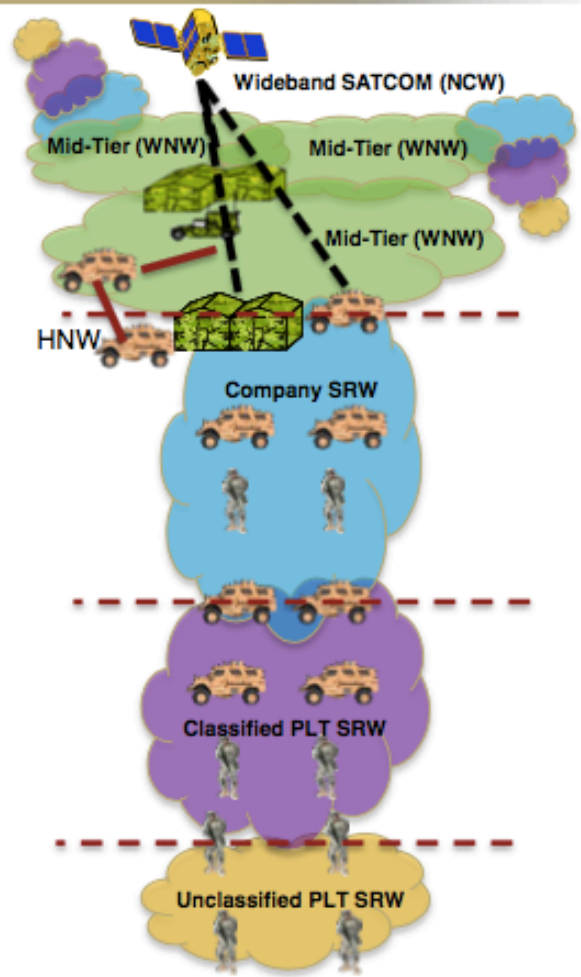


U.S. ARMY RDECOM

Communications-Electronics Research, Development and Engineering Center (CERDEC)

– Challenge Areas –

CERDEC US ARMY – RDECOM



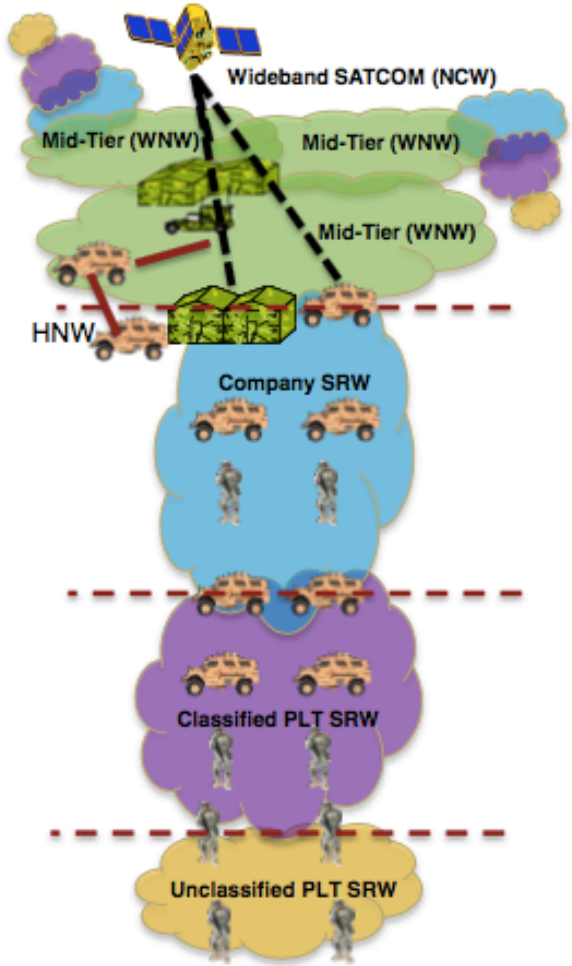
- **Operational Complexity (OC)** – while the network is extremely complex, it should not be operationally complex nor should it be complex to use. The Tactical Internet (TI) is too complex (using manual and static methods) to configure. The TI needs control algorithms to be able to adapt to demands placed upon it by mission (e.g., mobility), by data dissemination (e.g., applications) and by policy for all deployment scales.
- **Limited Throughput to Tactical User (LT)** – given our current deployment engineering rule, our LTI platoon radio networks provide limited per-user throughput. This throughput limit needs to be increased.
- **RF Interference (RFI)** – systems within the Tactical Internet need better integration for improved SWAP and simplification of operation within the Tactical Internet. Robust waveforms must be maintained and improved to meet future jamming challenges and future LPI/LPD requirements in the presence of Blue EW and Red EW.
- **Non-Convergence on Tactical Internet (NC)**– the Army's prominent tactical applications require improved network services for full integration on our IP-based Tactical Internet.
- **Dis-contiguous Architecture (DA)** – the architecture has developed through multiple acquisitions.

SoS Challenges Characterized into These Broad Problem Areas

U.S. ARMY RDECOM

Communications-Electronics Research, Development and Engineering Center (CERDEC)
– Focus Areas Towards Improvements –

CERDEC US ARMY – RDECOM

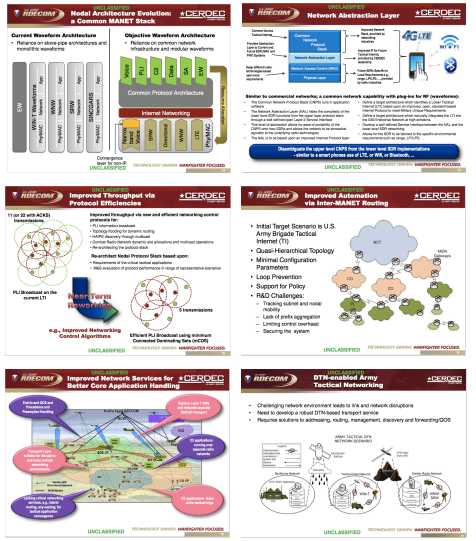


- **Simplify Management and Operations**
  - Common data models
  - Common management protocols
  - Move towards improved automation, e.g., new control protocols
  - Promote Mobile Ad-Hoc Network (MANET) standards
- **Refocus on Robust Basic Capabilities**
  - Robust Voice, PLI and limited C2 to the soldier
  - Improved LPI/LPD operation in denied environments
- **Modularize the Architecture**
  - Common network protocol layers
  - Swap-able MAC/PHY 'waveforms'
- **Improve Frequency Efficiency**
  - Better frequency reuse and coordination between RF systems
  - Frequency agile RF systems

Improve the core network services and capabilities

CERDEC architectural and technology improvements

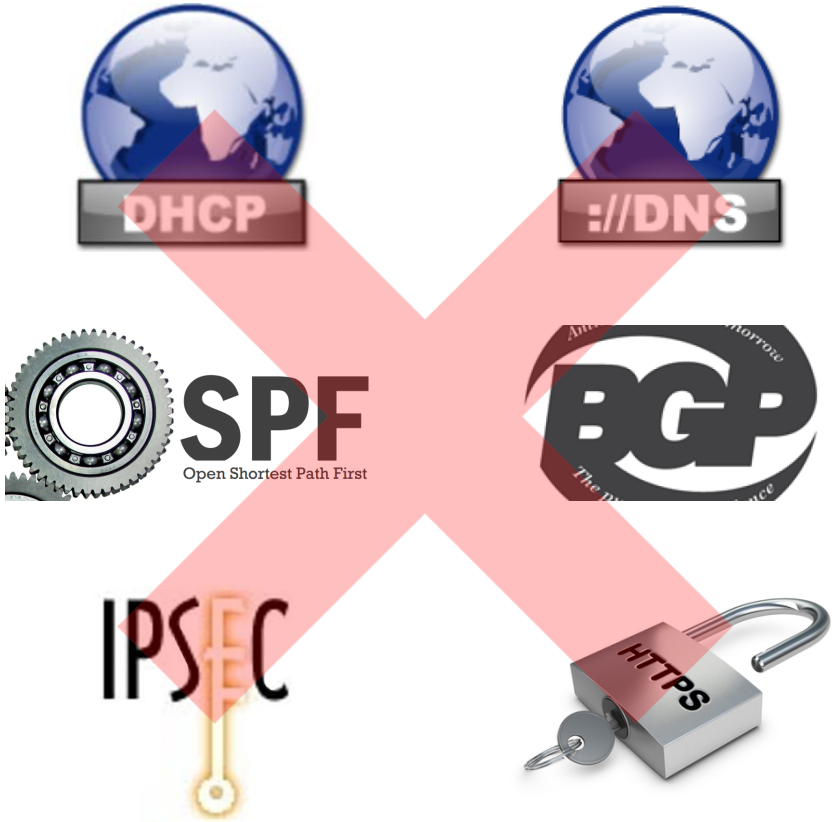
- A common MANET stack (to replace stove-piped approach)
- Improved throughput, protocol efficiency, and automation (loop-free routing, low overhead)
- Disruption tolerance



How can NDN contribute towards these objectives?

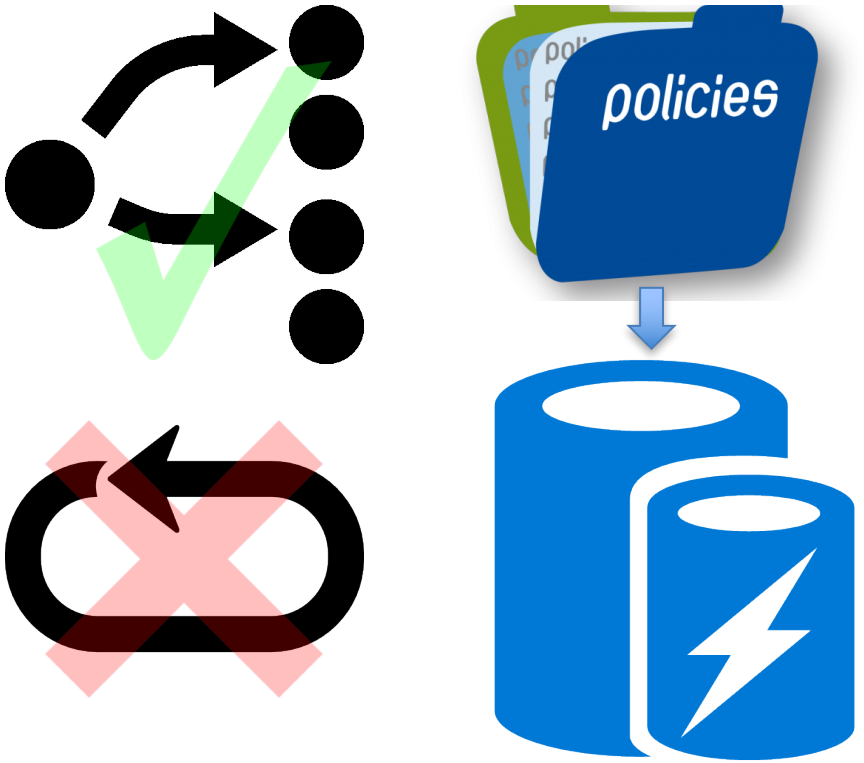
NDN simplifies the tactical networks

- No need for complex host-centric routing and addressing services
- No need for overlay security services
- Application semantics exposed to the network



NDN improves the effectiveness of tactical networks

- Robustness, resiliency, and scalability are core NDN features
  - Policy-based caching and forwarding strategies (delay, disruption, and/or mission aware)
  - Multicast support is organic
  - Loop-free routing is guaranteed



NDN improves the efficiency of tactical networks

- Storage is cheaper than bandwidth
- Policy-based caching strategies (delay, disruption, and/or mission aware)
- Minimizes control traffic

NDN improves security

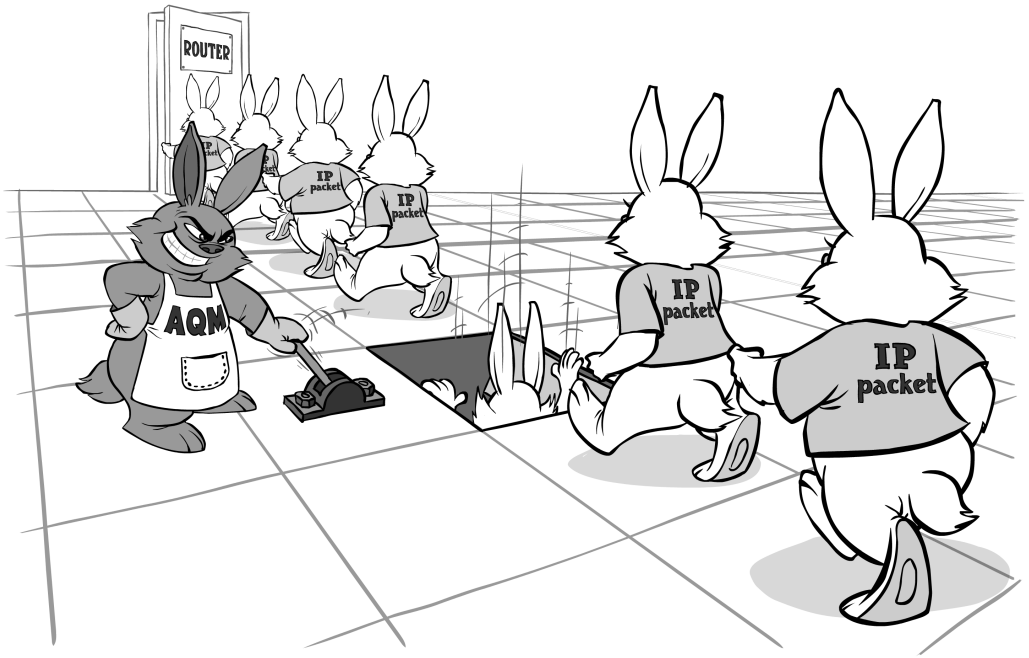
- Name-based filtering: filtering applied to the data directly
  - Ingress Interest/Data packet filter based on names

/sensors/aircraft-1111/HD-pic

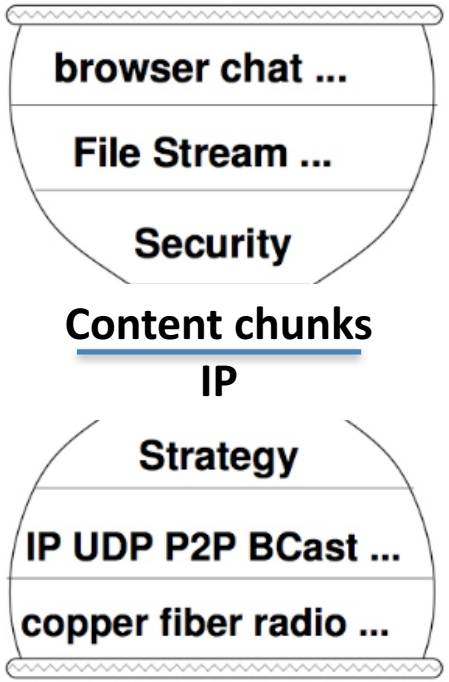
/sensors/aircraft-1111/HD-video

NDN improves security

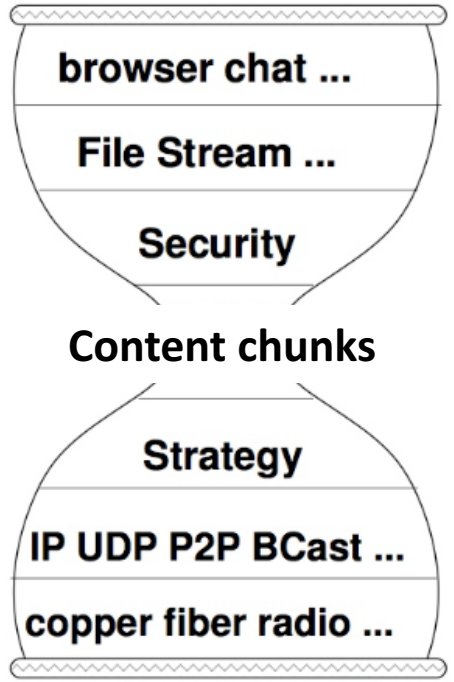
- Data secured at rest and in-transit
- Data-centric security is more resilient than securing channels
  - Loss on a VPN channel has dramatic impact on its stability (DARPA SHARE)
- Scalable key distribution



NDN's role in future tactical networks

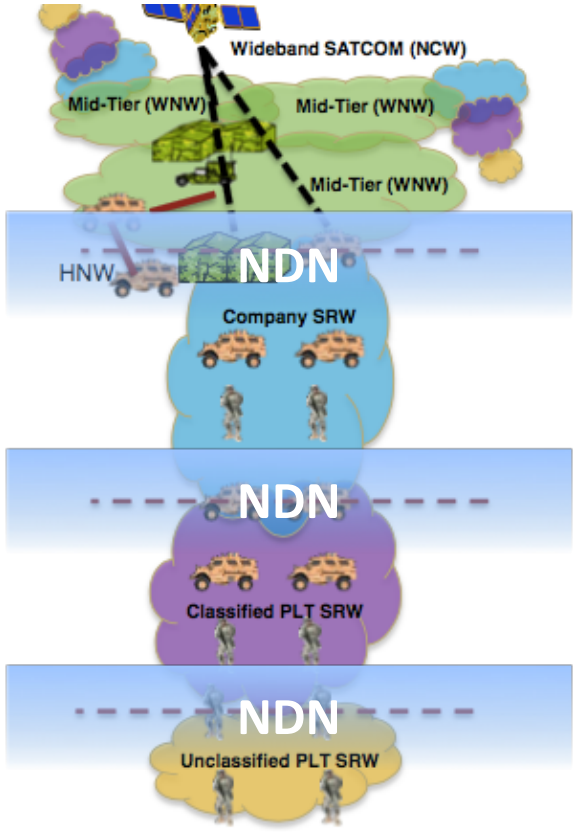


- NDN as the thin-waist of the hour glass
  - Clean-slate approach (long-term)
- NDN interoperable with existing infrastructure (short-term)



NDN's role in future tactical networks

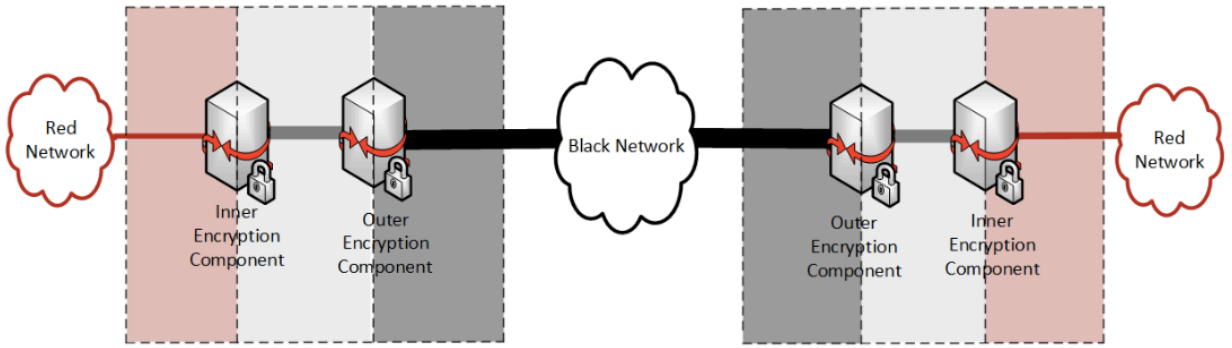
- NDN gateways separating network partitions
  - Where disruption is likely to occur
  - Where delay is likely to be high
  - Where bandwidth is low
- Tuned caching and forwarding policies



What problems do we need to solve?

- Operation in ciphertext networks
- Legacy architecture using HAIPEs
  - Same problem existed for DTN
  - CDS solutions
  - Name obfuscation is possible

- CSfC compliant operation
  - Layer 1: NDN producer
  - Layer 2: NDN forwarder (face)



What problems do we need to solve?

- Event-driven applications
  - NDN is consumer driven
  - Some applications are triggered by producer
- Name-based QoS policies
- Data perishability
- Confidentiality

Conclusion

- NDN is already being evaluated in tactical networks
- NDN data-centric communication paradigm addresses a lot of the communication/security challenges in today's tactical networks