FNC3 CHALLENGES

- DoD requirements for network capabilities (both at the enterprise and tactical edge) continue to rapidly expand and evolve, as **targeted data sharing at the speed of relevance** has become one of the prime differentiators on the battlefield.

- Future DoD networks will need to manage **higher volumes of data, larger numbers of users, and more diverse mission sets** across DoD, including coordination with the commercial sector, other U.S. government agencies, and international allies.

- These requirements will **stretch the limits of existing DoD network infrastructure**. In order to achieve the network capabilities described above, DoD will need to expand the capacity and flexibility of its networks.

    - Network capacity can be improved by adding more physical infrastructure to increase bandwidth (e.g., buying more storage), transitioning to faster physical infrastructure (e.g., upgrading from broadband to fiber), or finding ways to use existing resources more efficiently (e.g., using existing infrastructure more flexibly and/or using a proxy cache).

    - Network flexibility can be improved by abstracting control and user planes above the physical hardware to maximize efficient use of existing hardware, or by acquiring more dedicated network hardware to accommodate different user preferences. While this second approach can provide more options for users, it will also add to the burden of network administration unless it adopts a more flexible hardware management strategy, such as the abstraction method of the first approach.

- DoD must increasingly depend on commercial sector network technologies for large swaths of its networks as commercial sector leads the charge in developing cutting edge network technologies. As a result, **DoD must improve its approach to integrating commercial network solutions.**

- The commercial sector has already developed a range of hardware and software solutions to improve network capacity and flexibility, but **DoD is currently not well-positioned to take advantage of these commercial solutions.**

    - Hardware: installing and maintaining physical infrastructure is expensive and time-consuming. These cost and time challenges are exacerbated for DoD due to the dispersed and disparate nature of physical infrastructure across various DoD networks, as well as their varied acquisition strategies and funding priorities.

    - Software: DoD still treats software much like hardware, and often misunderstands the relationship between speed and security. As a result, a large amount of DoD's software

takes too long, costs too much, and is too brittle to be sustainable in the long run. For a more thorough analysis of DoD software challenges and suggested remedies, please see the Defense Innovation Board's Software Acquisition and Practices (SWAP) Study.[1]

FNC3 OPPORTUNITIES

- DoD should consider a two-pronged approach to improving its use of commercial solutions:
    - 1. Improve network resource management by increasing network capacity and flexibility, and shift DoD mindset toward "communication networks as a platform or a service," to include tactical communications
    - 3. Develop a DoD-wide network strategy to enable organizations to synchronize network development efforts and maximize interoperability
- DoD should invest in methods to make the best use of existing network infrastructure capacity. Options can range from virtualization of servers, desktops, and network functions to maximize hardware use, software defined networking to control packet flow throughout the network, network slicing to provide more flexible network experiences for users, and other methods that have already been tested and deployed on networks across the commercial sector.
- In the long term, DoD must invest in network infrastructure to increase network capacity, while bearing in mind future requirements to build in excess capacity as needed. While DoD can take some steps to improve the efficiency of existing network infrastructure to maximize its use, it cannot constantly operate at the outer limits of its network capacity: its missions are too critical to bear the risk of communications failure or delay.
- Overall, DoD must take a more intentional and strategic approach to evaluating and integrating commercial solutions into its networks, modifying them as needed for military environments. DoD must first improve its awareness of existing state-of-the-art commercial solutions to understand the world of the possible, then build out a long-term strategy for network architecture and design. Once a strategy is in place, DoD can then seek out commercial products that fit its strategy where appropriate and coordinate acquisition and integration of those products across the organization.

Existing DoD data and communications networks suffer from numerous shortfalls. Broadly, DoD lacks a modern network architecture, adequate security in the face of increasing vulnerabilities, and connectivity and interoperability at the intra-Service, inter-Service, and inter-generational system levels. This ultimately prevents theatre commanders from achieving maneuver and engagement flexibility in contested environments, and makes it harder for new technologies like hypersonic weapons and hypersonic defenses to be deployed. The Services have and are continuing to develop their own network infrastructure and architecture concepts, but have not taken a unified approach to ensure interoperability. Current military data transfer systems on their own do not adequately provide the resilience, reach,

[1] J. Michael McQuade and Richard M. Murray, "Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage," Defense Innovation Board, 3 May 2019, https://innovation.defense.gov/software/.

bandwidth, modularity, and security required for the future battlefield. Some of these problem sets are unique to DoD networks and missions, but many have partial or full solutions that have already been developed in the commercial world. DoD leadership will be better positioned to achieve its optimal "battle network" if it has more visibility into existing commercial network solutions and leverages those solutions where appropriate to enhance existing networks and build future ones.

Ultimately, DoD should aspire to integrate "state of the art" commercial network technologies into its networks at the speed of relevance. Commercial sector is increasingly leading the charge in innovative network architecture and design, and these commercially-derived technologies play an increasingly critical role throughout DoD operations. However, there are a number of barriers to overcome before DoD can fully leverage commercial sector offerings in the field of network architecture. **DoD is currently not well-positioned to take advantage of cutting edge network technologies available in the commercial world.**

DoD must address two key barriers if it hopes to position itself for better acquisition and integration of commercial solutions in its networks. First, DoD must manage the restrictions on its network resources, from flexible usage to total available bandwidth. DoD network infrastructure is aging, outdated, and expensive, and DoD network usage is rapidly outgrowing its network capacity. Second, DoD must manage its cultural approach to communications networks. The current method narrowly assesses network capacity demand for each organization in the near term, which drives most DoD networks to operate near maximum capacity with redundancies across one another. Instead, DoD should adopt a "communications as a platform" approach, assessing aggregate demand on networks in order to buy capability more effectively and efficiently with a comprehensive, long term vision of network architecture in mind. DoD will have a better foundation to sustain commercial solutions once it has addressed these challenges, but it will still need a coordinated plan of attack to successfully buy and implement those solutions. Organizations across DoD should keep track of "state of the art" commercial solutions and synchronize their efforts to build interoperable networks.

These recommendations complement the "DoD Digital Modernization Strategy," in which DoD CIO has set out a roadmap to support implementation of the National Defense Strategy lines of effort through the lens of cloud, artificial intelligence, command, control, and communications, and cybersecurity. In particular, these recommendations may be used in support of the Digital Modernization Strategy's third goal to "Optimize for Efficiencies and Improved Capability."[2]

[2] *DoD Digital Modernization Strategy*, DoD CIO, 12 July 2019, https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF.

DIB FNC3 RECOMMENDATIONS

1. NETWORK RESOURCE MANAGEMENT

Recommendation 1.1: Maximize efficiency and capacity of existing physical infrastructure across DoD networks.

- Deploy traditional commercial sector best practices for optimizing bandwidth (e.g., quality of service (QoS) protocols, traffic grooming).
- Virtualize functions on existing DoD servers and data centers, and require future network components to include virtualization technology. Move toward Network Function Virtualization (NFV) by building in a federated control/orchestration mechanism for virtualized network functions, leveraging and managing virtualized servers across the network.[3] For a more comprehensive overview of NFV, please see Appendix A (NFV section).
- Monitor network traffic flow to identify patterns and bottleneck points, automate network resource allocation by time and task to account for those patterns and bottlenecks.
- Centralize network traffic management via Software Defined Networking (SDN) to clear paths for higher priority packets and adjust resources accordingly to hierarchically optimize network traffic. For a more comprehensive overview of SDN, please see Appendix A (SDN section).
- Virtually segment the network into "slices" that are individually optimized for different user requirements. This method of network slicing separates the user plane from the control plane and moves the user plane toward the network edge, while management functionality remains at the core. Network slicing relies on network function virtualization to run multiple network slices on the same set of hardware, then optimizes each slice to the configuration preferences of each user. For a more comprehensive overview of network slicing, please see Appendix A (network slicing section).
- These methods of managing network capacity should help DoD organizations become comfortable with aggregating their networks. Network owners may initially hesitate to relinquish control over bandwidth and packet prioritization, but these methods will improve capacity and allow those owners to feel that there is room for surge capacity in the network if needed.

Recommendation 1.2: Invest in new network infrastructure with future network capacity requirements in mind.

- While DoD can and should improve its existing network capacity using efficiency mechanisms described in Recommendation 1.1, DoD must also invest with future network use in mind, which will require DoD to buy more physical infrastructure that will provide more bandwidth.
- Additionally, DoD should continue to invest R&D and coordinate with private sector to develop and implement 5G ecosystems that prioritize security both in and out of the United States. 5G will increase DoD's ability to link multiple systems into a broader network while sharing

[3] https://ribboncommunications.com/company/media-center/blog/how-company-can-implement-network-function-virtualization-nfv-their-network

information in real time, improving communication across Services, geographies, and domains while developing a common picture of the battlefield to improve situational awareness.

**See the DIB's 5G Study[4] for more context on 5G risks and opportunities for DoD.*

Recommendation 1.3: Better defend network resources by moving to a "zero trust" security architecture.

- Zero Trust Architecture (ZTA) has the ability to fundamentally change the effectiveness of security and data sharing across DoD networks. From a security perspective, ZTA can better track and block external attackers, while limiting security breaches resulting from internal human error. From a data sharing perspective, ZTA can better manage rules of access for users and devices across DoD to facilitate secure sharing, from the enterprise center to the tactical edge. As DoD networks continue to expand and Zero Trust Architecture (ZTA) can significantly offset vulnerabilities and threats across DoD networks by creating discrete, granular access rules for specific applications and services within a network.

- Network design and flexibility of ZTA would also help DoD more rapidly adopt and implement critical network technologies and enablers, ranging from cloud computing to artificial intelligence and machine learning.

**See the DIB's Zero Trust Architecture (ZTA) White Paper[5] and Recommendations[6] for more context on potential ZTA implementation across DoD.*

Recommendation 1.4: Support existing "connect-a-thons" and encourage more of them throughout DoD to allow more systems and platforms be linked, with an emphasis on cross-domain and cross-Service interoperability.

- The Air Force is already investigating the "connect-a-thon" concept to increase links between systems and platforms, using Advanced Battle Management System (ABMS) as the connective tissue.[7] DoD should encourage all Services to continue pursuing these efforts to improve connectivity across the Department.

- Focus should be on cross-domain and cross-Service interoperability in order to leverage service specific network investments and reduce redundant, isolated systems.

COMMERCIAL SOLUTIONS INTEGRATION

---

[4] Milo Medin and Gilman Louie, "The 5G Ecosystem: Risk & Opportunities for DoD," Defense Innovation Board, April 2019, https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF.
[5] Kurt DelBene, Milo Medin, and Richard Murray, "The Road to Zero Trust (Security)," Defense Innovation Board, 9 July 2019, https://media.defense.gov/2019/Jul/09/2002155219/-1/-1/0/DIB_THE_ROAD_TO_ZERO_TRUST_(SECURITY)_07.08.2019.PDF.
[6] Zero Trust Recommendations to be published, deliberated, and voted on at 31 October 2019 public meeting.
[7] Theresa Hitchens, "EXCLUSIVE: Air Force To Upgrade ABMS Every 4 Months: Roper," *Breaking Defense*, 18 September 2019, https://breakingdefense.com/2019/09/exclusive-air-force-to-upgrade-abms-every-4-months-roper/.

Recommendation 2.1: Assign responsibility within the Department to develop and deploy DoD Network Architecture Strategy to provide coordinated path forward for DoD entities buying commercial solutions.

- OSD should designate a single entity in DoD to synchronize network commercial product acquisition, using a broader Network Architecture Strategy as a guide to determine whether and what commercial products and/or technologies are appropriate to integrate into DoD networks. Each product or technology should be considered in the context of a future desired DoD network endstate to better assess its value in the near and long term.

- This approach should allow Services to coordinate their network acquisition efforts and find time and cost efficiencies in network usage, rather than taking multiple different, disconnected approaches while buying commercial solutions on an "as-needed" basis.

Recommendation 2.2: Stand up DoD-Commercial Liaison Office to interface with commercial sector and build a knowledge base of "state of the art" commercial solutions for DoD to leverage.

- DoD is frequently years, if not decades, behind commercial sector in technology implementation, and will likely continue to lag commercial sector in certain technology fields. However, by maintaining an awareness of "state of the art" in the commercial sector, DoD leaders can understand the realm of the possible and integrate technologies with an understanding of future opportunities, particularly in the field of network solutions.

- The Liaison Office should serve as a resource for DoD entities to leverage when evaluating commercial solutions, and should also proactively reach out to DoD to maintain a common understanding of commercial solutions available. The Liaison Office should release regular reports on new developments in various industries and technologies and coordinate regularly scheduled "Education Days" to keep DoD leadership informed about new technical concepts coming out of the commercial sector.

- The Liaison Office should establish a regular presence at industry events, conferences, and round tables. This will allow the office to stay current on developing trends and technologies, and can also serve as an interface point to familiarize commercial sector with DoD and improve DoD-technology sector relationships.

APPENDIX A:

SUMMARY

- Commercial industry has already begun implementing a variety of best practices, both for network design and network usage, that enable more efficient and flexible network performance. Key practices include:
    - **Network Function Virtualization (NFV)**,
    - **Software Defined Networking (SDN)**, and
    - **Network Slicing**
- **NFV** gets more "bang for your buck" out of network physical resources by simulating each physical resource in software, allowing users to **maximize resources** without having to buy new dedicated hardware to increase network capacity.
- **SDN** drives **more efficient flow of network functions** by abstracting a "control plane" above those functions and using that federated control to improve flow and efficiency across the network.
- **Network slicing** virtually segments the network into "slices" that are individually optimized for different user requirements. This allows for **more deliberate and targeted network usage based on the required QoS and priorities of the user**.
- In combination, these key practices enable enterprises to better use hardware, operating systems, and applications on a network while accounting for differing functional preferences of users. These benefits are critical to DoD and its networks going forward, as user requirements will continue to become more diverse and complex.

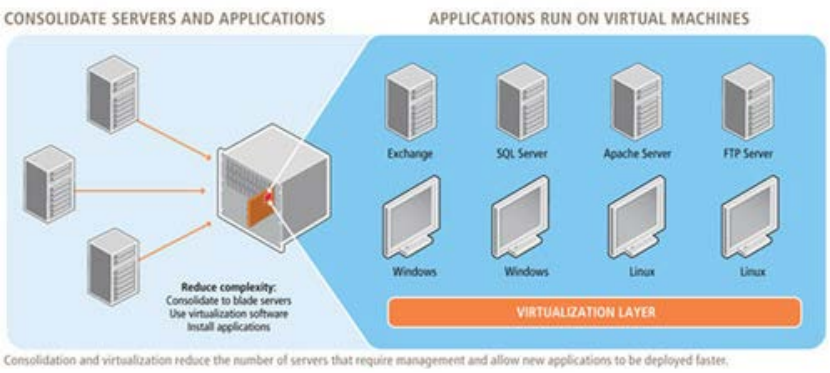
FUTURE NETWORK ARCHITECTURE: STARTER'S KIT

Network Function Virtualization (NFV)

NFV gets more "bang for your buck" out of network resources by simulating each physical resource in software, allowing for more flexible resource usage without having to buy new dedicated hardware for each network function.[8] To better understand virtualization and how it can be applied to network functions, consider the following analogy.

Carol, Bob, and Jill all need transportation (some specific network resource). They each would prefer to have their own vehicle to travel to their distinct locations, but it is ultimately expensive and inefficient for each of them to buy their own (duplicative fuel costs, empty seats, increased traffic, etc.).

Instead of separate cars, it would be more efficient to transport Carol, Bob, and Jill on a single mode of transportation (carpool). This conserves time, space, and other resources while still providing Carol, Bob, and Jill with transportation.



Consolidation and virtualization reduce the number of servers that require management and allow new applications to be deployed faster.

Additionally, in the virtualization version of this analogy, we can still provide Carol, Bob, and Jill with the *virtual experience* of having their own individual transportation that goes directly to their destination of choice while still transporting them in a single car. Carol, Bob, and Jill may be sitting in the same car in reality, but they will still feel as though they have the car to themselves without additional stops or delays due to carpooling.

Just as the carpool allows multiple people to transport in the same car, virtualization allows multiple users to run on top of the same network resource. Virtualization uses software called "virtual machines" (also known as "VMs," or "hypervisors") to manage and direct allocation of the resource to the different users that previously required their own distinct sets of hardware (separate cars). This method allows hardware to be used at its full capacity instead of wasting a large percentage of its resources by only allowing for one user or application at a time.[9]

While virtualization can be applied to multiple discrete network resources (e.g., servers, operating systems, desktops), network function virtualization (NFV) specifically separates out multiple resources required for network functionality (such as directory services, file sharing, and IP configuration) to be

[8] Rashid Mijumbi, et al, "Network Function Virtualization: State-of-the-art and Research Challenges," IEEE, 4 September 2015, https://ieeexplore.ieee.org/document/7243304.
[9] Songlin Sun, et al, "Integrating network function virtualization with SDR and SDN for 4G/5G networks," IEEE, 1 June 2015, https://ieeexplore.ieee.org/abstract/document/7113226.

packaged and redistributed among users.[10] NFV may consist of one or more virtual machines running different software and processes, on top of standard high-volume servers, switches and storage devices, or even cloud computing infrastructure, instead of having custom hardware appliances for each network function. This reduces the number of physical switches, routers, servers, cables and other hardware across a broad number of users, driving down the cost and effort of increasing network capacity.[11]

Implications for DoD

- Physical network resources are expensive and time-consuming to add/replace in a network.
- DoD in particular struggles with adding new physical network infrastructure because of the size and diversity of its networks: increasing network capacity through physical infrastructure would require the addition of a larger number of physical devices.
- NFV provides a path around this challenge by using existing physical infrastructure more efficiently, allowing more users to ride on the same hardware.
- Pockets of DoD currently employ virtualization for servers, desktops, and other hardware, but DoD has yet to deploy virtualization for network functions
- Commercial sector has deployed NFV, but commercial networks are largely homogenous and static, whereas DoD networks are heterogeneous and non-static, with significantly less fiber on which they can rely.
- NFV offerings are currently concentrated in a relatively small number of vendors. In the long term, DoD may want to consider the health and diversity of the "network industrial base," in addition to its traditional defense industrial base, as DoD increasingly relies on dual-use commercial sector offerings to build its network capabilities.
- NFV will enhance the warfighter by allowing more users to run on existing infrastructure. It will also reduce infrastructure costs, freeing up funding for other critical warfighting requirements

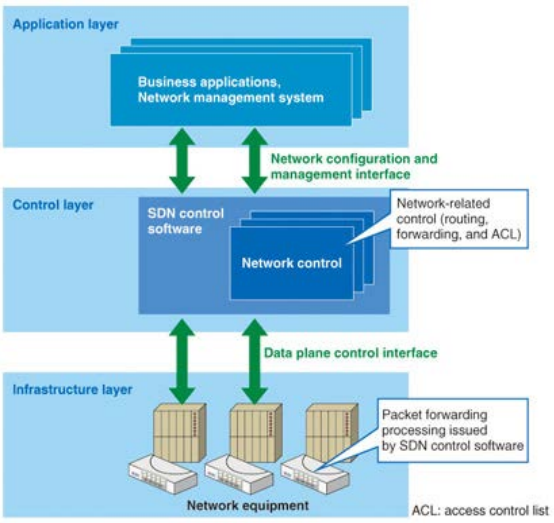
[10] Margarte Chiosi, et al, "Network Functions Virtualisation: An Introduction, Benefits, Enablers, Challenges & Call for Action," SDN and OpenFlow World Congress, 22 October 2012, https://portal.etsi.org/nfv/nfv_white_paper.pdf.
[11] Yong Li and Min Chen, "Software-Defined Network Function Virtualization: A Survey," IEEE, 9 December 2015, http://www.ece.ubc.ca/~minchen/min_paper/SDN-NFV2015.pdf.

Software Defined Networking (SDN)

SDN drives more efficient flow of network functions by abstracting a "control plane" above those functions and using that centralized control to improve flow and efficiency across the network.[12]

Returning to our previous example: Carol, Bob, and Jill are on the road, either carpooling in a single car or driving their own individual cars (NFV is recommended but not required for SDN). They share the road with hundreds of other cars, all trying to get to their own distinct destinations (network packet flow). However, instead of each car taking a predetermined route each time and risking traffic congestion with other cars on the same route, it would be more efficient to have a centralized "route manager" that controlled all cars and could manage the flow and congestion of traffic throughout the city by automatically shifting cars to different streets and routes to optimize the flow of the entire city (network). This route manager could also assign prioritization to certain cars who needed to get to their destinations faster, optimizing paths around those priorities.

Just as a route manager would improve the flow of traffic throughout a city, SDN can improve the flow of packets throughout a network by creating a control plane distinct from the data plane.[13] While the control plane makes decisions about how packets should flow through the network, the data plane actually moves packets from place to place. Where a traditional network would use a specialized appliance, such as a firewall or load balancer, SDN replaces the appliance with an application that uses the controller to manage data plane behavior.[14]



In a classic SDN scenario,[15] a packet arrives at a network switch, and rules built into the switch's proprietary firmware tell the switch where to forward the packet. These packet-handling rules are sent to the switch from the centralized controller. The switch (also known as a data plane device) queries the controller for guidance as needed, and it provides the controller with information about traffic it handles. The switch sends every packet going to the same destination along the same path and treats all the packets the exact same way. SDN uses an operation mode that is sometimes called "adaptive" or "dynamic," in which a switch issues a route request to a controller for a packet that does not have a specific route.

---

[12] Hyojoon Kim and Nick Feamster, "Improving Network Management with Software Defined Networking," IEEE, February 2013, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.413.1407&rep=rep1&type=pdf.
[13] Diego Kreutz, et al, "Software-Defined Networking: A Comprehensive Survey," IEEE, 8 October 2014, https://arxiv.org/pdf/1406.0440.pdf.
[14] Bruno Nunes, et al, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," IEEE, 13 February 2014, https://ieeexplore.ieee.org/abstract/document/6739370.
[15] Margaret Rouse, "Software Defined Networking (SDN)," TechTarget, August 2019, https://searchnetworking.techtarget.com/definition/software-defined-networking-SDN.

The virtualization aspect of SDN comes into play through a virtual overlay, which is a logically separate network on top of the physical network. Users can implement end-to-end overlays to abstract the underlying network and segment network traffic.[16]

Implications for DoD

- DoD networks must manage a growing amount of data traffic flowing between a growing number of endpoints.
- SDN can help deconflict DoD network traffic and reducing latency in data transfer by improving network efficiency and implementing policy-driven network supervision.
- SDN also creates an opportunity to improve DoD network security by providing a federated point that can monitor and log traffic, as well as distribute common security policies throughout the network. This will also help DoD efforts to shift to a "zero trust" least-privilege access model by creating better awareness of network mapping and standardizing security policies.
- SDN can also reduce overall DoD network administration costs by centralizing and automating many network management functions.
- SDN will enhance the warfighter by identifying critical packets on the network and speeding up the rate of data transfer for high priority missions and environments.

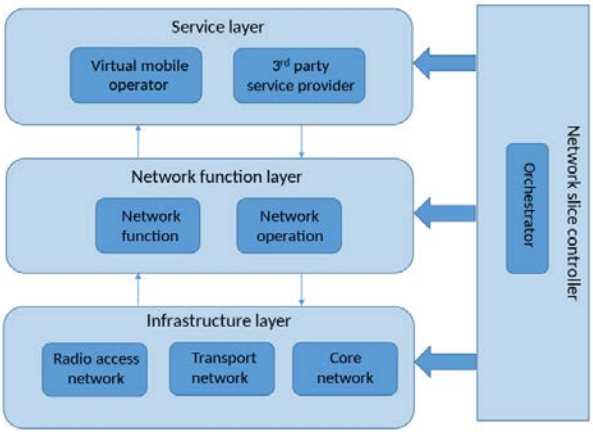
[16] Soheil Hassas Yeganeh, "On scalability of software-defined networking," IEEE, 14 February 2013, https://ieeexplore.ieee.org/abstract/document/6461198.

Network Slicing

Network slicing virtually segments the network into "slices" that are individually optimized for different user requirements. This allows for more deliberate and targeted network usage based on the preference of the user. Just as SDN separates the control plane from the data plane, network slicing separates the user plane from the control plane and moves the user plane toward the network edge, while management functionality remains at the core.[17] Network slicing relies on network function virtualization to run multiple network slices on the same set of hardware, then optimizes each slice to the configuration preferences of each user.

Returning to our example with Carol, Bob, and Jill: all three are using the same car, but have the virtual experience of having their own car using NFV, and their movement across the network is optimized using SDN. However, each person has specific preferences for their type of transportation (network configuration) that may differ from one another: for example, Carol may care more about storage space, Bob may care more about fuel efficiency, and Jill may care more about speed.

In this virtualized environment, Carol can be given a virtual truck to maximize storage space, Bob can be given a virtual bicycle to maximize fuel efficiency, and Jill can be given a sports car to maximize speed, while all three continue to ride in the same physical vehicle (network hardware). Rather than forcing all three to use the same configuration that may not be optimized for any of their requirements, network slicing provides each user with a virtual "network slice" that provides more intentional allocation and configuration of network resources.



Network slicing provides dedicated networks to users without requiring dedicated hardware by running multiple end-to-end logical networks on top of the same hardware.[18] Network slicing includes physical resources, but can also include logical resources (such as management functions, VPNs, etc.). These logical networks can host multiple users that share common preferences for their networks, or single users with highly specific preferences. These preferences can span the range of latency, data security, mobility, throughput, and others, and network slicing can selectively optimize for any of these priorities.

Network slicing is frequently discussed in the context of 5G, as it will enable improved mobility and roaming across operators and enable broader use cases like IoT.[19] The larger volume of users and user

[17] "An Introduction to Network Slicing," GSM Association,2017, https://www.gsma.com/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introduction-to-Network-Slicing.pdf.
[18] Ibrahim Afolabi, "Network Slicing and Softwarization: A Survey on Principles, Enabling Technologies, and Solutions," IEEE, 21 March 2018, https://ieeexplore.ieee.org/abstract/document/8320765.
[19] Haijun Zhang, et al, "Network Slicing Based 5G and Future Mobile Networks: Mobility, Resource Management, and Challenges," IEEE, 9 August 2017, https://ieeexplore.ieee.org/abstract/document/8004168.

connections associated with 5G will have a more diverse range of network preferences, all while running on multiple networks run by multiple operators. In this context, network slicing will allow for more efficient, precise, and flexible network usage.

Implications for DoD

- DoD network users have diverse network preferences that are dependent on factors ranging from mission to location to types of individual users interacting with the network.
- Physical network resources are expensive and time-consuming to add/replace in a network: DoD in particular struggles with adding new physical network infrastructure because of the size and diversity of its networks, and increasing network capacity through physical infrastructure would require the addition of a larger number of differently configured physical devices.
- Some commercial players have implemented network slicing, but commercial networks are able to rely on a more modern and advanced network architecture that already employs virtualization and SDN, whereas DoD must play catch-up on those network architecture fundamentals to be able to implement network slicing.
- To mitigate concerns over network capacity availability across networks and slices, DoD can set minimum guaranteed capacity for each slice that remains constant regardless of usage elsewhere in the network. This will require capacity planning and simulation to understand excess capacity requirements in the event that multiple parts of DoD's network ecosystem must surge usage simultaneously.
- Network slicing will enhance the warfighter by allowing DoD to work with its existing physical network infrastructure, while providing more flexibility for the preferences of its users.