The Rise of IPv6

Benefits and Costs of Transforming Military Cyberspace

Dr. Panayotis A. Yannakogeorgos

Maintaining awareness of advancing technology and harvesting the opportunities it creates is in our blood as innovative Airmen. . . . Pursuit of the next "game changing" technology is central to maintaining the asymmetric advantage our Air Force has always provided the nation.

—Secretary of the Air Force Deborah Lee James

As the US Air Force prepares for an age of strategic agility, we become excited with headline-grabbing emerging technologies such as hypersonic aircraft, nanotechnology, and remotely pi-

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
APR 2015		**00-00-2015 to 00-00-2015**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Rise of IPv6: Benefits and Costs of Transforming Military Cyberspace	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Research Institute (AFRI),Air and Space Power Journal,155 N. Twining Street,Maxwell AFB,AL,36112**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**26**	

loted and autonomous systems that will in time become core mission enablers.[1] Too often overlooked are the invisible transmission control protocol (TCP) / Internet protocol (IP) networking protocols that revolutionized the military and the world by changing how humans exchange and use information. This networking protocol enhances and enables the Air Force's five core missions: air and space superiority; intelligence, surveillance, and reconnaissance (ISR); rapid global mobility; global strike; and command and control.

Secretary of the Air Force Deborah Lee James notes in the recent strategy document *America's Air Force: A Call to the Future* that "this strategy challenges our Air Force to forge ahead with a path of strategic agility—breaking paradigms and leveraging technology just as we did at our inception."[2] Today, the Department of Defense (DOD), Air Force, and nation are focused on technologies important to future development. However, unbeknownst to many people, the structure of the Internet is changing for the first time in its history with the exhaustion of the IP version four (IPv4) protocol and the adoption of IPv6. The DOD—as well as the Air Force in particular—has a tremendous opportunity and responsibility to lead the nation in the transition to IPv6 to enhance and enable core functions and missions, assuring that our cyber operators are educated and trained to keep pace with technological change.

A recent report by the DOD inspector general found several missteps on the part of the department's chief information officer (CIO), US Cyber Command, and the Defense Information Systems Agency in terms of making IPv6 a priority. A lack of coordination and failure of the CIO to maintain a plan of action, together with milestones for transition to IPv6, have cost the DOD time and will increase expenses.[3] Over the course of an 18-month-long cyber workforce-development study, the Air Force Research Institute discovered several worrisome trends and perceptions that contributed to an environment in which IPv6 was not a top national security priority that it should be. This article outlines why it should have higher priority and why operators

and senior leaders alike should be worried about the slow pace of IPv6 migration within the DOD.

The department researched and developed the Advanced Research Projects Agency Network (ARPANET), which eventually became the Internet, when it transitioned the ARPANET from network control protocol (NCP) to TCP/IP in 1981. The DOD led the world in developing and deploying the core protocols and standards by which applications and services were delivered to users. Today the core of the Internet, cyberspace's most potent manifestation, is about to change for the first time in history, and we are not in the lead. The TCP/IP communications protocol, a scarce, critical Internet resource, is transitioning from IPv4 to IPv6. The latter will introduce features into the networking environment, such as quality of service and multicasting that will enhance how information is used and exchanged. Voice over IP and television over IP are but two applications that stand to benefit from IPv6 and will revolutionize how the world communicates in the same way that satellites have.[4] The need to transition from IPv4 to IPv6 is not hypothetical since the global supply of IP addresses in IPv4 is quickly being exhausted (fig. 1).[5]

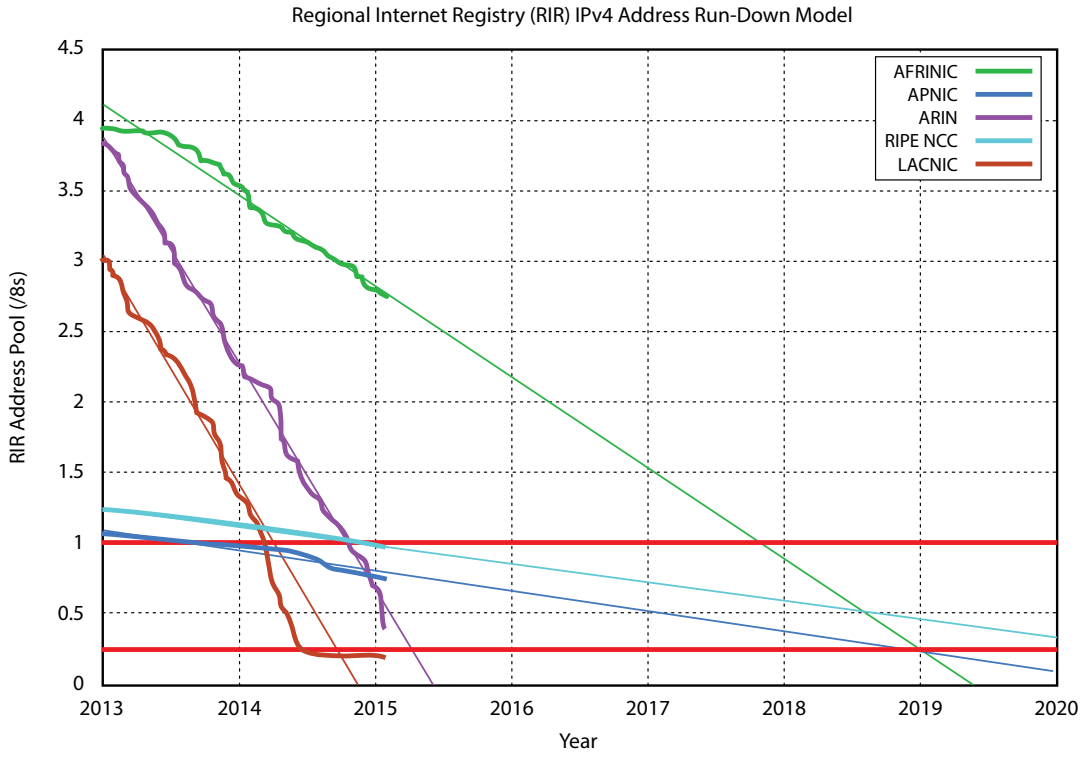

Figure 1. Projection of consumption of remaining regional Internet registry address pools. (From "IPv4 Address Report," accessed 29 January 2015, http://www.potaroo.net/tools/ipv4/. This report generated 29 January 2015, 08:07 UTC. Reprinted with permission.)

AFRINIC - African Network Information Center

APNIC - Asia Pacific Network Information Center

ARIN - American Registry for Internet Numbers

RIPE NCC - Réseaux IP Européens Network Coordination Centre

LACNIC - Latin American and Caribbean Network Information Center

Internationally, calls for transitioning to IPv6 have been ongoing since 1996 and have intensified with the 2013 "Montevideo Statement" of the Internet Corporation for Assigned Names and Numbers (ICANN) calling the "transition to IPv6 to remain a top priority globally. In particular Internet content providers must serve content with

both IPv4 and IPv6 services, in order to be fully reachable on the global Internet."[6] It will require more than just a flip of a switch for the DOD and the Air Force to transition. It will demand significant resources and commitment to the educating and training of our cyber workforce to preserve the missions in this evolving domain upon which the DOD relies so heavily.

What Is an IP Address, and Why Do We Need It?

Machines identify each other on the Internet and most networks by means of IP and media access control (MAC) addresses. Although invisible, IP addresses are finite in number, making them a scarce and critical Internet resource. All networked hardware and software must have a valid IP and address to function on a network, whether the open Internet or a closed sensor-control network. In particular they identify machines, guiding data packets and information across computer networks—including the Internet. The use of data packets, the basic units of network traffic, is the standard method of dividing information into smaller units when it is sent over a network. A vital component of networks, the IP header, contains information pertaining to the source and destination addresses. Machines require these strings of numbers to connect with other computers on the Internet or other networks.[7] Data packets are re-created by the receiving machine based on information within a header of each packet that tells the receiving computer how to re-create the information from the packet data. Without standardized communications protocols, such as TCP/IP, there would be no assurance that packets could be read by a receiving machine.[8]

As more people, organizations, and machines cross the digital divide, IP addresses become depleted as they are allocated by service providers. The processes for assigning scarce IP addresses and allowing the Internet to serve as a global platform are complex. ICANN allocates IPv4 address space to various registries via the Internet Assigned Numbers Authority (IANA) in agreement with the US National Tele-

communications and Information Administration of the US Department of Commerce, which currently retains stewardship over the procedural role of administrating changes to the Domain Name System (DNS) root-zone file.[9] The IANA allocates address space in the size of /8 prefix blocks (16,777,216 IP addresses) for IPv4 to requesting regional registries as needed.[10] The regional Internet registry (RIR) then resells smaller /16 blocks (64,000 IP addresses) to Internet service providers (ISP) and other organizations. ISPs then resell smaller blocks of IP address space to end users to access the Internet (fig. 2). The allocation of IPv6 addresses is similar; however, it is structured so that all IPv6 networks have space for 18,446,744,073,709,551,616 IPv6 addresses. In layman's terms, each network will have more space than the entire IPv4 pool.[11]

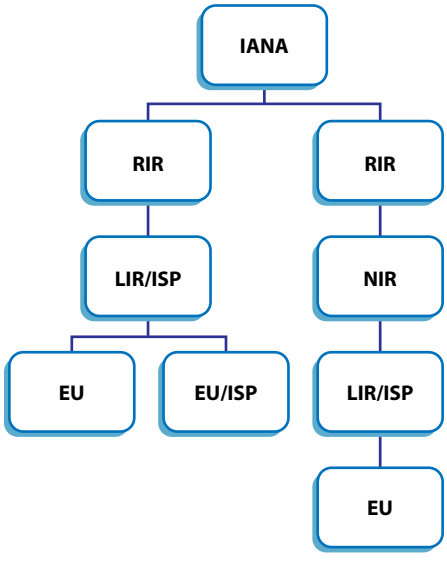

Figure 2. Current address allocation hierarchy

IANA: Internet Assigned Numbers Authority

RIR: regional Internet registry

LIR: local Internet registry

ISP: Internet service provider

NIR: national Internet registry

EU: end user

Unlike the popular conception of a limitless Internet, the underlying address space is finite. Indeed, IPv4 address space has already run out for allocation by IANA and RIRs in Europe, Asia, and Latin America. Foreseeing this eventuality, engineers developed IPv6 in the 1990s. Among other improvements, it increased the total number of potential IP addresses from 4,294,967,296 in IPv4 to 2^{128} in IPv6.[12] Although the IPv6 protocol has been deployable since 1996, today the world faces a shortage of IPv4 address spaces on which the Internet currently relies. This deficit will only become worse as the establishment of an "Internet of things" intensifies. As machines begin communicating with other machines, each will require its own IP address. ICANN noted in 2011 that "future expansion of the Internet is now dependent on the successful global deployment of the next generation of Internet protocol, called IPv6."[13] Although CIOs within the DOD and US government acknowledge that the world is transitioning from IPv4 to IPv6 as the dominant communications protocol for the global Internet, it is not evident that rapid transition is a priority.

The Air Force's Road to Migration

Within the service, the Air Force Network Integration Center (AFNIC) has been working on the Air Force's transition from the current IPv4 addressing format to IPv6 since 2002. The latest transition deadline received a soft mandate of 2014.[14] In reality, however, Air Force migration will take much longer, based on the fact that the service has not begun migrating the core network service capabilities except at selected bases. Even those that have started have since rolled back their efforts.[15] Other than a few labs and the Defense Research and Engineering Network, no more than a half dozen machines on the live Air Force Nonsecure Internet Protocol Router (NIPR) Network are legitimately using IPv6.[16] Even so, it has been noted that the plan involves using both IPv4 and IPv6 in parallel for the next 10–15 years. This approach further complicates operational success because the dual framework creates an additional energy load on processors to run both

protocols, potentially negating some of the benefits of a complete transition. Further, it introduces vulnerabilities into the system.

What Are the Military Benefits of Transition?

In his foreword to *America's Air Force: A Call to the Future*, Gen Mark A. Welsh III, the Air Force chief of staff, emphasizes that "the Air Force's ability to continue to adapt and respond faster than our potential adversaries is the greatest challenge we face over the next 30 years."[17] Certainly, an entire article can be written about the fact that China is leading the world in operational deployment of IPv6-only networks through its China Next Generation Internet program.[18] The effects on US national security could be substantial.[19] The ability of foreign actors to begin dominating the field of Internet governance poses a tremendous problem to our current security environment. However, addressing such threats lies beyond the scope of this article. This section concerns itself less with the threat than with the utility of deploying IPv6 native networks and the potential vulnerability of not doing so without a strategy to educate our cyber workforce in this new operating environment.

For both the DOD and the Air Force, IPv6 is a critical technology for enabling network-centric warfare theories in support of all five of the service's core missions. In addition to the basic number of IP addresses available, IPv6 allows for more advanced networking capabilities than does IPv4. Networked machines/sensors, devices, applications, and services will benefit from improved functionality with IPv6. Indeed, the outcome of the Air Force chief scientist's *Cyber Vision 2025* study suggests several technologies that would greatly benefit from the expansive address space that IPv6 offers. Adopting widespread use of the protocol would prove especially beneficial in the areas of assuring and empowering the mission, as well as enhancing agility and resilience of the systems dependent on cyber capabilities. IPv6 benefits could be leveraged to reduce cyber risk to Air Force missions by enabling IP hopping; morphable architectures; agile, tactical communica-

tions; heterogeneous, operationally responsive networks; and other crosscutting mission areas. *Cyber Vision 2025* acknowledges these benefits of IPv6.[20] However, current CIO strategies call for the transition to full IPv6 to occur with IPv4/IPv6 dual stacking in phases.[21] Dual stacking or the running of IPv4/IPv6 in parallel is a bad idea. First, it introduces well-documented security vulnerabilities.[22] Do we expect that our potential adversaries will not understand this fact and fail to leverage the advantages of IPv6, thus challenging our efforts in the cyber domain? Second, it increases manpower costs since the workforce must understand both.

IP address space is important for delivering the elements of all of the Air Force's core missions. Allocations are occurring all the time, and large programs demand substantial allocations. One example that illustrates this point within the global-mobility mission set involves the new KC-46 tanker aircraft currently on an assembly line that is expected to produce 179 aircraft over the next 20 years. All of them need IP address space. Every Air Force mission must have large IP address spaces per platform to support a robust and redundant communications platform that requires multiple network switches to ensure resilient command and control as well as mission objectives.

Another example highlighting the advantages regards flexible, global integrated ISR capability as called for in the Air Force's strategy document: "Expanding requirements and a growing threat to high cost air-breathing assets will also necessitate a shift from an architecture focused on dedicated ISR platforms to one based on a diverse network of sensors arrayed across the air, space, and cyber domains, placing a premium on the ability to draw data from any and all US systems."[23] The expanded address space would allow for a massive number of sensors networked together in a vast IP address space that would give sensors their own static IP addresses. Further, communications devices with their own static IP address running solely IPv6 would consume less energy, thus providing longer-lasting battery life in mobile

devices on which the command and control of many military operations depend.[24]

Why Have We Not Converted Yet?

Persistent myths continue to hamper discussions about transitioning to IPv6.[25] Primarily they fall into four categories: (1) immature architecture, (2) security vulnerabilities, (3) the myth that the DOD has a sufficient allocation of IPv4 addresses, and (4) the fiscal burden of conversion during a time of austerity.

Immature Architecture

Some people assert that the v6 arena has not matured enough to force a change that includes technology, architecture, and the skills of operations personnel. One view within the Air Force holds that there are no compelling drivers to IPv6 at this time and that the cyber operations community has more than enough on its plate for now. However, this argument falls flat on its face on two points. First, the US government CIO and Government Accountability Office, as noted above, encourage dual stacking. Second, the Air Force strategy declares that "one of the most important responsibilities of a military service is to prepare the force for the challenges of tomorrow, not just the realities of today."[26] It is also clear that although most information technology (IT) equipment is IPv6 capable, the Air Force does not have any substantial plans to make use of this capability in the foreseeable future (two to five years).[27] At present, the greatest operational challenge is making sure that new capabilities to tunnel v6 over v4 and vice versa are turned off so that our adversaries cannot exploit them.[28]

Security Vulnerabilities

A key future challenge is that even if v4 and v6 are enabled during a transition period, the National Institute of Standards and Technology (NIST) notes that "prevention of unauthorized access to IPv6 networks

will likely be more difficult in the early years of IPv6 deployments."[29] Indeed, contrary to conventional wisdom, serious security vulnerabilities exist that go beyond turning on IPv6 on the networking equipment that the Air Force has already purchased. NIST warns,

> As the IPv6 protocol becomes increasingly ubiquitous, all enterprise and Internet-connected networks need to be prepared for specific threats and vulnerabilities that the new protocol will bring. For example, an IPv4-only network segment may contain several newly installed hosts that are both IPv4 and IPv6-capable, as well as hosts that have IPv6 enabled by default. This circumstance can come about simply as a result of the normal systems life cycles. Additionally, IPv6 could be enabled on a host by an attacker to circumvent security controls that may not be IPv6-aware; these hosts can then be leveraged to create covert or backdoor channels. Taken further, IPv6 traffic could be encapsulated within IPv4 packets using readily available tools and services and exchanged with malicious hosts via the Internet.[30]

Implications include that many host-based defense and forensics tools can't handle the large address space of IPv6 networks. The smallest IPv6 subnet will be 4 billion times larger than the entire IPv4 range; consequently, defenders will have difficulty finding victims. An IPv6 scanner could take days or weeks to locate all the hosts on the Air Force network, let alone actually scan them for vulnerabilities. Existing IPv4 intrusion detection systems cannot inspect the contents of an IPv6 tunneled packet and vice versa. Thus, a financial cost will be associated with acquiring the systems to defend v4 and v6 networks. This is in addition to the cost to educate and train our cyber operators, who will need additional education and training as well as the establishment of network defense tools to detect the potential threat of exactly the opposite of tunneling IPv4 over IPv6. Hence, although going dual stack everywhere is an admirable goal, realistically, doing so will have an effect on each of the tunneling protocols on the throughput, data rates, and latency that result.

Myth That the Department of Defense Has a Sufficient Allocation of IPv4 Addresses

Another erroneous perception pervading the discussion touts that IPv4 depletion is not a problem for the DOD since a large allocation of IPv4 addresses worldwide has already been reserved for national security purposes.[31] Historically, the DOD has been a repository of technical expertise regarding the Internet, given the latter's roots within the Defense Advanced Research Projects Agency; its operation of the ".MIL," a top-level domain for exclusive use by the DOD; and its running DNS name servers to support it. In the early 1990s, the DOD acquired a significant amount of the IPv4 space—12 blocks of /8 block space. With each /8 block containing 16,777,214 IP addresses, the DOD has over 200 million addresses available in v4 space. The current situation with IPv6 is analogous to that of IPv4 in the early 1990s. The DOD has purchased a /13 block of v6 space, the equivalent of 42,000,000,000,000,000,000,000,000,000,000,000,000 IP address spaces.[32]

Conventional wisdom across much of the Air Force is that the DOD and the Air Force have no reason to worry about IP address depletion. Indeed, only a very small percentage of the Air Force network uses any IPs from those 12 allocations. Huge chunks of that network predate the assignment of those /8 networks, and it skews the DOD projections if one assumes that those 12 /8 networks are all that are available to work with. Thus, an accurate analysis will consider the true IPv4 addresses that the Air Force is using, most of which were directly acquired before the DOD received its big allocations.[33] Calculations on the publicly available DOD Network Integration Center "WHOIS" database reveal that the department has slightly more than 317 /16 networks currently listed as reserve networks that have been recovered for future assignment.[34] A mixture of smaller allocations also exists. Of the 317 /16 networks, currently one unused /8 network (29.0.0.0/8) is being held in reserve. If the purpose of doing so is to support the entire DOD, then that is not adequate address space for future applications.

Within the Air Force, annual averages of the IPv4 rate of depletion do not clearly show a trend for increasing or decreasing burn rates (fig. 3). Anomalous numbers in 2010 were caused by network cleanup that fixed long-standing problems and really should be considered an outlier. Using these numbers on a linear exhaustion path, one finds that the projected exhaustion date of all currently Air Force–owned IP address space is Monday, 31 December 2029, although this is more likely to occur prior to that date because of increasing demands of IP address space as new systems go online that demand more of this limited resource. Thus, the notion that the DOD and the Air Force do not need to worry about IPv4 depletion is a myth. Planning for the inevitable conversion must start sooner rather than later since allies will likely run out of IPv4 address space well before 2029.

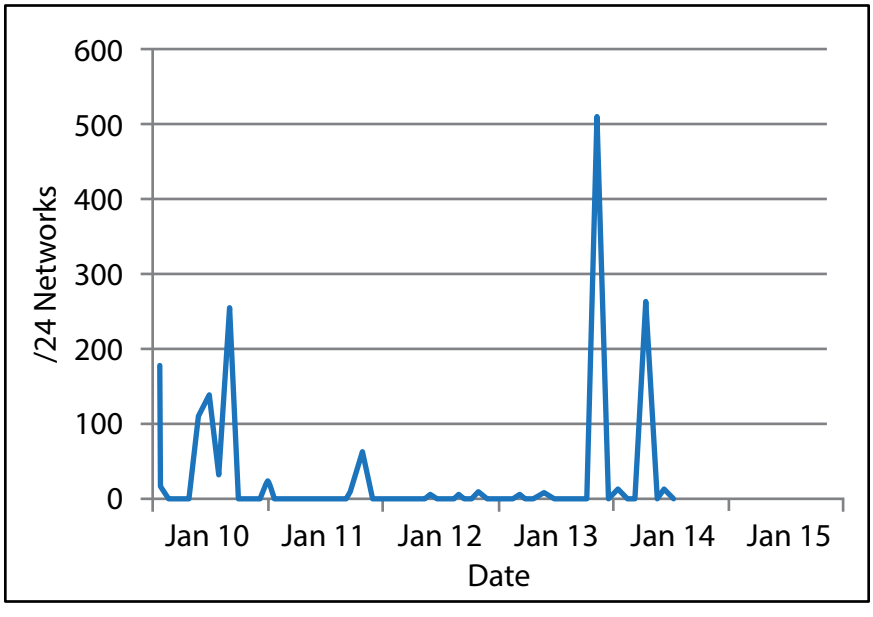

Figure 3. Number of /24 networks assigned per month, Nonsecure Internet Protocol Router

The Air Force's *Call to the Future* document is unambiguous in its belief that coalition warfare will continue to be critical to the success of the service over the next 30 years: "Indeed, the most likely and most demanding scenarios involve the Air Force working in concert with, or leading, coalition Airmen."[35] Assuredly, this prospect is already a challenge.[36] If and when partner and allied nations shift their domestic and military networks to IPv6, then interoperability between our networks and allied/coalition networks will not be possible without transition or translation techniques between the two protocols. This situation will increase vulnerability to operational missions. To mitigate this vulnerability, NIST recommends in its *Guidelines for the Secure Deployment of IPv6* that the best practice is to block all IPv6 traffic on IPv4-only networks.[37]

IPv6 penetration is increasing worldwide, including in the United States.[38] However, the DOD is not keeping pace because of the perception that having many IPv4 addresses allocated to the .MIL domain does not necessitate the transition. To remain interoperable, the DOD will need to be on IPv6 and able to work with full IPv6 systems in the future. It takes a long time to plan deployment and train operators to successfully employ and defend a new system. Thus, we need to start sooner rather than later.

Fiscal Burden of Conversion during a Time of Austerity

Finally, individuals who oppose a rapid conversion to IPv6 also raise the issue of a financial burden associated with transition. Admittedly, additional funds will be required to cover the cost of new infrastructure and network services. Therefore, according to critics, in a budget-constrained environment with competing priorities, it is not the right time to conduct the transition. This argument is partly true. Because the DOD pioneered the Internet, the United States owns a very large legacy infrastructure that is IPv4. Thus, the cost of transitioning will be higher than that of most other organizations that do not have a legacy infrastructure. Nations and organizations with little infrastructure

will be able to start directly on IPv6-compatible infrastructure utilizing methods such as dual stacking during the transition period and then shutting off IPv4. However, the AFNIC has been an advocate for IPv6 since 2002. Using the tools at hand and emphasizing strategies focused on buying IPv6-capable equipment were refreshed during the normal tech refresh cycle since 2003 when the DOD required all hardware and software "developed, procured or acquired shall be IPv6 capable (in addition to maintaining interoperability with IPv4 systems/capabilities)."[39] The National Defense Authorization Act also includes an IPv6 inspection element for the Air Force's CIO to use as a metric for each program's score cards: "The PM [program manager] shall initiate efforts to transition IPv4 systems and applications to support IPv6 and determine the IPv6 impact. The PM shall conduct an analysis to determine cost and schedule impacts necessary to modify the system. The PM shall include IPv6 requirements in program acquisition and technology refresh budget and POM [program objective memorandum] submissions."[40] A bad mark on this report card could hold up funding for a program.[41] Federal acquisition regulations also direct that IPv6 equipment be obtained for any purchase after December 2009 when the IPv6 requirement came about.[42] Figures 4–6 show the status of IPv6 enablement across both the Air Force and the DOD.

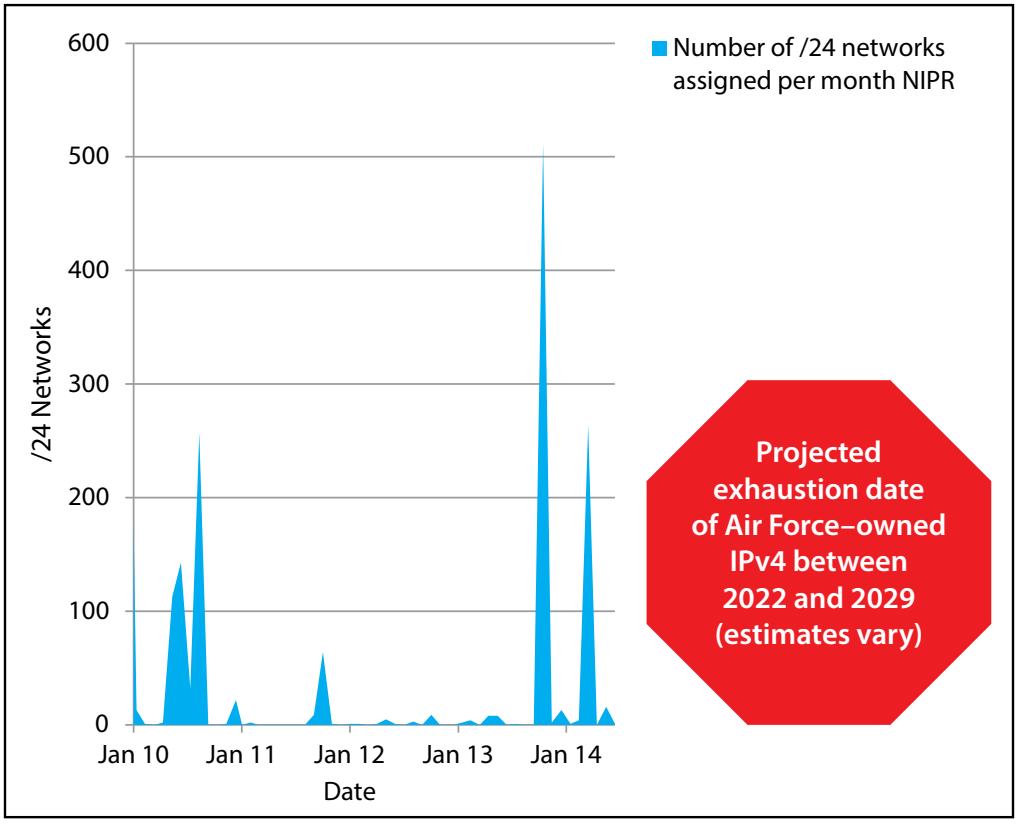

Figure 4. Number of IPv4 networks assigned per month. (Reprinted from data provided by the Air Force Systems Networking office.)

NIPR - Nonsecure Internet Protocol Router Network

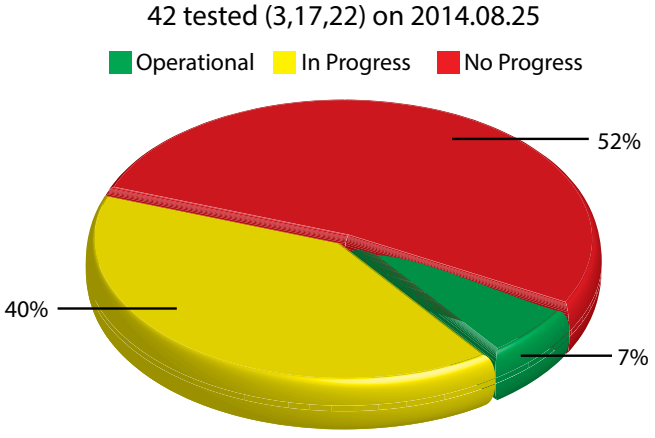

Figure 5. Completed IPv6 enabled domains, Department of Defense. (Reprinted from "Estimating IPv6 & DNSSEC External Service Deployment Status, Department of Defense," Information Technology Laboratory, Advanced Network Technologies Division, National Institute of Standards and Technology, accessed 2 February 2015, http://fedv6-deployment.antd.nist.gov/cgi-bin/cfo?agency=defense.)

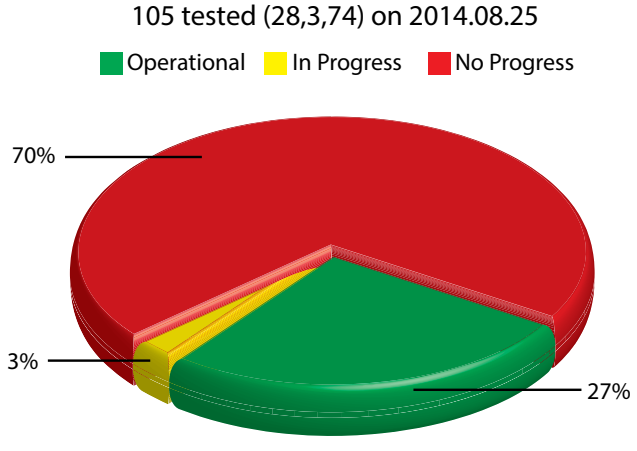

Figure 6. IPv6 enabled services, Department of Defense. (From "Estimating IPv6 & DNSSEC External Service Deployment Status, Department of Defense," Information Technology Laboratory, Advanced Network Technologies Division, National Institute of Standards and Technology, accessed 2 February 2015, http://fedv6-deployment.antd.nist.gov/cgi-bin/cfo?agency=defense.)

Thus, in accordance with the acquisition regulations, the equipment has been purchased during tech refresh cycles. As new devices, appliances, and additional infrastructure are purchased and old equipment is replaced, all new equipment must be IPv6 capable—and that has not been an issue. The DOD, however, has fallen behind in applications and systems that are not IPv6 capable. The AFNIC must work with the Air Force Business Enterprise System to develop a path forward for implementing IPv6 compliance for all digital services and applications that will harness the benefits of IPv6 in military operations.

Despite the few (if any) equipment costs, one cannot argue that IPv6 transition involves no expenses. If the Air Force and DOD continue down the current path, it is almost certain that more financial hardships will occur due to manpower requirements; specifically, the Air Force and DOD will need two staffs of network administrators and so forth—one IPv4 trained and the other IPv6 trained. Indeed, in an *IPv6 Economic Impact Assessment*, NIST estimated the cost of training one person on the high end as $2,906, with total costs much higher (see the table below).[43] Indeed, the same report indicates that the more accelerated the transition to IPv6, the more expensive it becomes.

Table. Summary of transition costs from IPv4 to IPv6

	Costs (Present Value Millions $2003)[a]
Infrastructure vendors	$1,384
Application vendors	$593
ISPs	$136
Users	$23,321
Total	$25,434

[a] Calculated using a 7 percent real social discount rate

Source: Reprinted from Michael P. Gallaher and Brent Rowe, *Planning Report 05-2, IPv6 Economic Impact Assessment* (Washington, DC: NIST, US Department of Commerce, Technology Administration, October 2005), ES-4, http://www.nist.gov/director/planning/upload/report05-2.pdf.

Recommendations

Mandate a Firm Transition Date to IPv6 Utilizing DOD Acquisition Policies and the Joint Information Environment

Currently the level of commitment and willingness to take risk and begin a migration of services into the Air Force environment does not exist. The DOD has a forgotten history of protocol conversions. When the ARPANET was first deployed, it was not TCP/IP based but relied on an implementation of NCP. On the basis of additional research from 1973 to 1981, TCP/IP was developed to allow for improvements to the existing packet-switched networks, allowing "internetworking" to emerge as a network architecture—hence, the Internet was "born." Indeed, the *NCP/TCP Transition Plan* proclaimed in November 1981 that "the Department of Defense has recently adopted the internet concept and the IP and TCP protocols in particular as DoD wide standards for all DoD packet networks, and will be transitioning to this architecture over the next several years. All new DoD packet networks will be using these protocols exclusively."[44] The transition to TCP/IP was successful only because of the firm mandate. Specifically, the *NCP/TCP Transition Plan* mandated "a complete switch over from the NCP to IP/TCP by 1 January 1983. It is the task of each host organization to implement IP/TCP for its own hosts. This implementation task must begin by 1 January 1982."[45]

Air Force leadership must enforce a similar mandate today. Firm transition dates have been attempted with IPv6 in the past—for example, in an order by the Office of Management and Budget (OMB) in August 2005, and again on 28 September 2010 another OMB memorandum mandated the federal transition to IPv6.[46] The Air Force acknowledged that the transition should take place but did not solidly establish an actual command emphasis on the effort. The most forceful requirement was the August 2005 OMB memo that actually included dates that everybody attempts to ignore. Thus, without emphasis from the Air Force A6/CIO mandating a firm date for migration

with penalties for noncompliance, the migration has little chance of full implementation.

The time is ripe today to implement this migration throughout the DOD. Corresponding with the development and deployment of the joint information environment (JIE), "in order to facilitate implementation of JIE through acquisition across the Department, new IT programs will be required to comply with the JIE. Existing IT programs will be mandated to address JIE requirements as they progress through their lifecycle, and decisions will be made on how they can best comply with the JIE."[47] Indeed, the DOD has directed the completion of this migration no later than the end of fiscal year 2018.[48] Critics might argue that the reliance on IPv4 is stronger today and more integrated into day-to-day military operations. Though that statement is true, development of the JIE offers the DOD-CIO office an opportunity to pause this effort and include language aligning JIE net readiness with a mandatory IPv6 implementation plan to transition the JIE to IPv6 by the end of fiscal year 2018. Doing so will go a long way to ensure that the DOD has IPv6 hosts enabled and services deployed, enabling the paradigm shift to the IPv6 environment. Thus, assuming that JIE is fielded sometime before 2030, the DOD and the Air Force should not have any issues running out of IPv4 address space before migrating to JIE and IPv6.

Educate and Train Our Cyber Operators in IPv6

Today the Air Force cyber schoolhouses offer some general background on IPv6 in the curriculum—in the best case, two hours of instruction. This amount is not sufficient. Detailed, specific training on IPv6 should be required, but some people believe it is not needed since it does not represent current operational reality.[49] Instead, the preference is to reserve that type of training for future cyber field training units that will catch up operators on the latest advances in our actual capabilities as they move between assignments. This reasoning is perilous since in cyber operations, experience matters. As noted

briefly above, our Chinese competitors, among others, are gaining experience in operating IPv6 networks while the Air Force ignores the problem. To resolve this dilemma, the service should begin by educating and training future cyber warriors in IPv6 as soon as the Air Education and Training Command (AETC) and Air Force Space Command (AFSPC) curriculum design processes allow.

Important elements that should be included in a training tasking letter from career field managers and Twenty-Fourth Air Force to AETC and AFSPC education and training units include, but are not limited to, curriculum updates covering the following specific elements of IPv6 that are prone to vulnerabilities when employed:

- multicast listener discovery/enumeration;
- router discovery/enumeration;
- node querying;
- user datagram protocol (UDP)/TCP checksum calculation;
- transition mechanisms 6to4, 6in4, 6over46rd, 4rd, Teredo, intrasite automatic tunnel addressing protocol (ISATAP);
- stateless address autoconfiguration (SLAAC);
- secure neighbor discovery protocol (SeND);
- neighbor discovery protocol;
- duplicate address detection;
- router, dynamic host control protocol (DHCP), and DNS discovery;
- redirection;
- new features in DHCPv6; and
- host and network mobility for the tactical, satellite, and aircraft systems.

Because cyber operations demand hands-on experience, this may involve considering additional funding and creating an IPv6 range both

at Keesler and Hurlburt Air Force bases where Undergraduate Cyber Training and the 39th Information Operations Squadron conduct training. Critics might counter that the curriculum does not include enough hours for both IPv4 and IPv6. However, given the interrelationship between IPv4 and IPv6, by teaching v6 we also would effectively be teaching v4. Furthermore, the Air Force must ensure that Airmen already in the career field get more exposure to v6. One short-term solution would entail encouraging enrollment in the Federal Virtual Training Environment as more long-term retraining solutions are developed by AETC and AFSPC.

Conclusions

Transitioning to IPv6 is not a hurdle too difficult to clear. It is neither an undeveloped nor untested technology. Rather, the transition remains a problem of policy disconnected from the technological realities. IPv6 migration should be a primary concern for our senior leadership, and it appears that only clear commitment and direction will spur the necessary transition. When this does occur, a strategy must be put in place to assure that this transition is not a hastily executed solution but one that has clear goals and road maps for the secure implementation of IPv6 throughout the Air Force. In terms of the DOD, the JIE is an excellent place to begin full deployment of IPv6 and avoid additional costs of delayed transition, including possible mission failure. Our cyber operators must begin training now in the operating environment in which they will certainly be immersed during the next decade. Protecting the network and developing the next generation of tactics, techniques, and procedures for cyber operations will allow for assured and rapid execution of core Air Force missions. Harnessing IPv6 is critical if the service is to remain the best equipped, trained, and most lethal force on the planet. ✪

Notes

1. The research was partially supported by Office of Naval Research Grant N000141310878 and the Department of Defense Minerva Research Initiative.

2. Headquarters US Air Force, *America's Air Force: A Call to the Future* (Washington, DC: Headquarters US Air Force, July 2014), 4, http://airman.dodlive.mil/files/2014/07/AF_30_Year_Strategy_2.pdf.

3. Michael Peck, "DoD Fumbled IPv6 Transition, IG Says," C4ISR&Networks, 5 December 2014, http://www.c4isrnet.com/article/20141205/C4ISRNET/312050009/.

4. Voice over Internet protocol (VOIP) applications, for example, running on IPv4 sometimes drop packets, causing communications to sound garbled. With the quality-of-service feature in IPv6, this problem would go away because each VOIP data packet is marked and delivered in a manner that prevents garbling of the data.

5. For daily reports on the current IPv4 exhaustion-rate status, visit "IPv4 Address Report," accessed 3 February 2015, http://www.potaroo.net/tools/ipv4/.

6. "Montevideo Statement on the Future of Internet Cooperation," Internet Corporation for Assigned Names and Numbers, 7 October 2013, https://www.icann.org/news/announcement-2013-10-07-en.

7. Elihu Zimet and Edward Skoudis, "A Graphical Introduction to the Structural Elements of Cyberspace," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 91–112. See also Robert E. Molyneux, *The Internet under the Hood: An Introduction to Network Technologies for Information Professionals* (Westport, CT: Libraries Unlimited, 2003), 85–86.

8. Molyneux, *Internet under the Hood*, 27. For the layperson, a good way to think about the importance of standardization in international telecommunications is how we connect to electrical distribution networks while we travel. Because electrical adapters are not standardized, travelers must get an adapter to plug their device into foreign sockets if that region is not compatible with the traveler's home region. With electricity comes the added danger of nonstandardized voltage and cycles. Therefore, travelers must also be aware of whether or not their device will burn out if connected to a 220-volt electrical network if the device is capable of receiving only 110 volts of energy.

9. The IANA function, currently part of a cooperative agreement with the US Department of Commerce, is in the early phases of a transition to ICANN, pending approval of a proposal to the NTIA by ICANN on the transition. "NTIA Announces Intent to Transition Key Internet Domain Name Functions," National Telecommunications & Information Administration, 14 March 2014, http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions.

10. "Making Internet Number Resource Allocations to Regional Internet Registries," IANA, accessed 3 February 2015, http://www.iana.org/help/inr-request-procedure. IANA distributes the IPv4 space in /8 blocks.

11. "Understanding IP Addressing," RIPE Network Coordination Centre, 22 April 2014, http://www.ripe.net/internet-coordination/press-centre/understanding-ip-addressing.

12. "Internet Protocol, Version 6 (IPv6) Specification," Internet Engineering Task Force, December 1998, http://tools.ietf.org/html/rfc2460.

13. "Available Pool of Unallocated IPv4 Internet Addresses Now Completely Emptied: The Future Rests with IPv6," ICANN, 3 February 2011, https://www.icann.org/en/system/files/press-materials/release-03feb11-en.pdf.

14. Katherine Kebisek, "AFNIC Prepares Air Force for IPv6 Transition," Air Force Space Command, 4 April 2011, http://www.afspc.af.mil/news1/story.asp?id=123249968.

15. E-mail exchange between the author and AFNIC personnel, 21 April 2015.

16. I am grateful to Air Force Systems Networking (AFSN) for this observation.

17. Headquarters US Air Force, *America's Air Force*, 5.

18. For example, the Chinese government reached a historic milestone of having a global event with a native IPv6 infrastructure during the 2008 Summer Olympic Games. During 1936 the Nazis broadcast the Olympics live worldwide.

19. Panayotis A. Yannakogeorgos, "Internet Governance and National Security," *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 102–25.

20. Mark T. Maybury, *Cyber Vision 2025* (Washington, DC: US Air Force Chief Scientist, 13 December 2012), 24, https://www.my.af.mil/gcss-af/USAF/AFP40/d/s6925EC1355090FB5E044080020E329A9/Files/editorial/00Cyber%20Vision%202025%20FINAL%203-21-13.pdf.

21. Strategy and Planning Committee, Federal Chief Information Officers Council, *Planning Guide/Roadmap toward IPv6 Adoption within the U.S. Government*, version 2.0 (Washington, DC: Strategy and Planning Committee, Federal Chief Information Officers Council, July 2012), https://cio.gov/wp-content/uploads/downloads/2012/09/2012_IPv6_Roadmap_FINAL_20120712.pdf.

22. Carlos E. Caicedo, James B. D. Joshi, and Summit R. Tuladhar, "IPv6 Security Challenges," *IEEE Computer* 42, no. 2 (February 2009): 36–42. See also Harith Dawood, "IPv6 Security Vulnerabilities," *International Journal of Information Security Science* 1, no. 4 (2012): 100–105.

23. Headquarters US Air Force, *America's Air Force*, 15.

24. Stephen Lawson, "IPv6 Can Boost Mobile Performance, Battery Life, Proponents Say," *Computer World*, 11 January 2013, http://news.idg.no/cw/art.cfm?id=96C2FD24-B840-8D62-606480F34A52909D.

25. The highlights in this section are a compilation of observations made over the course of 15 months during interviews in support of a study on cyber workforce development directed by the chief of staff of the Air Force (publication forthcoming from Air University Press) as well as research conducted during an Office of the Secretary of Defense Minerva project METANORM, a multidisciplinary approach to the analysis and evaluation of norms and models of governance for cyberspace.

26. Headquarters US Air Force, *America's Air Force*, 20.

27. Airman in Headquarters Air Force, Air Staff A6 and A3/6, unattributed interview by the author, 24 April 2014.

28. I use the term *tunnel* here to refer to the ability to access IPv6 networks via IPv4 (and vice versa).

29. Sheila Frankel et al., *Guidelines for the Secure Deployment of IPv6* (Washington, DC: National Institute of Standards and Technology, 2010), 2-6, http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf.

30. Ibid., 2-7.

31. Air Force senior leaders, officers, enlisted and civilian cyber operators, unattributed interviews by the author, 2013–14.

32. Data derived from "Ghost Route Hunter: IPv6 DFP Visibility," SixXS, accessed 3 February 2015, http://www.sixxs.net/tools/grh/dfp/.

33. I am grateful to the AFSN office for its comments and collaboration in producing this section.

34. To do the calculations, one may visit the DOD Network Integration Center (DODNIC) website and do a search for "DNIC-RNET [reserve networks]," which will bring up all networks that the DODNIC considers "returned networks" (the NIC uses "RNET" to annotate networks returned to the IP managers). This information changes daily, depending on what is issued on any day but nearly always decreases. See "Search NIC Whois For," accessed 3 February 2015, https://www.nic.mil/cgi-bin/whoisweb.

35. Headquarters US Air Force, *America's Air Force*, 13.

36. Chad C. Serena et al., *Lessons Learned from the Afghan Mission Network: Developing a Coalition Contingency Network* (Santa Monica, CA: RAND Corporation, 2014), http://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR302/RAND_RR302.pdf.

37. Frankel et al., *Guidelines*, 2-7.

38. *Akamai's State of the Internet* 7, no. 1 (Q1 2014): 3, http://www.akamai.com/dl/akamai/akamai-soti-q114.pdf.

39. John P. Stenbit, Department of Defense chief information officer, to secretaries of the military departments, memorandum, subject: Internet Protocol Version 6 (IPv6), 9 June 2003, [2], http://www.defense.gov/news/Jun2003/d20030609nii.pdf.

40. Air Force Instruction 63-101/20-101, *Integrated Life Cycle Management*, 7 March 2013, 87, http://static.e-publishing.af.mil/production/1/saf_aq/publication/afi63-101/afi63-101_20-101.pdf.

41. I am grateful to AFNIC/NES for these observations.

42. "Federal Acquisition Regulation; FAR Case 2005–041, Internet Protocol Version 6 (IPv6)," in *Federal Register* 74, no. 236 (10 December 2009), http://www.gpo.gov/fdsys/pkg/FR-2009-12-10/pdf/E9-28931.pdf.

43. Michael P. Gallaher and Brent Rowe, *Planning Report 05-2, IPv6 Economic Impact Assessment* (Washington, DC: NIST, US Department of Commerce, Technology Administration, October 2005), 4-5, http://www.nist.gov/director/planning/upload/report05-2.pdf.

44. John Postel, *NCP/TCP Transition Plan*, November 1981, 1, https://www.ietf.org/rfc/rfc801.txt.

45. Ibid., 2.

46. Vivek Kundra, federal CIO, White House Office of Budget and Management, to CIOs of executive departments and agencies, memorandum, subject: Transition to IPv6, 28 September 2010, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/transition-to-ipv6.pdf.

47. Department of Defense Chief Information Officer, *Joint Information Environment Implementation Guidelines* (Washington, DC: Department of Defense Chief Information Officer, 12 September 2013), 7, http://dodcio.defense.gov/Portals/0/Documents/JIE/20130926_Joint%20Information%20Environment%20Implementation%20Guidance_DoD%20CIO_Final_Document.pdf.

48. Ibid., 9.

49. E-mail exchange between the author and Headquarters Air Force A3/6, 24 April 2014.

Dr. Panayotis A. Yannakogeorgos

Dr. Yannakogeorgos (ALB, Harvard University; MS, PhD, Rutgers University) is a research professor of cyber policy at the US Air Force Research Institute, Air University, Maxwell AFB, Alabama. His expertise includes the intersection of cyber power, national security, and military operations; international cyber policy; cyber arms control; global cyber norms; and Eastern Mediterranean security. He was formerly a member of the faculty at the Rutgers University Division of Global Affairs and an adviser on the Middle East, including Iran, for the UN Security Council.