Strategy Research Project

DIVERSIFYING THE DEPARTMENT OF DEFENSE NETWORK ENTERPRISE WITH LINUX

BY

LIEUTENANT COLONEL SHERMAN LACOST
United States Army

USAWC CLASS OF 2010

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
12-03-2010	Strategy Research Project	

4. TITLE AND SUBTITLE

Diversifying the Department of Defense Network Enterprise with Linux

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lieutenant Colonel Sherman LaCost

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Lieutenant Colonel Charles Grindle
USAWC CIO

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Historically, the United States and its closest allies have grown increasingly reliant on the technological evolution of automated systems. Those automated systems have provided continued efficiency, advancement and profitability to organizations around the globe. Despite the evolutionary advancements and corresponding economic strength associated with technological automation, the United States and its allies find themselves now globally tied to automation in a quest for daily existence. Due to our national reliance on these systems, the areas showing the most advancement also represent the greatest vulnerability if penetrated. Recognizing the strategic value to this global problem, this paper will set the stage to identify changes needed for our current client enterprise. The effective introduction of the Linux operating system at the client level will increase security, foster collaboration across all branches of government and decrease the fiscal tail of our current client-server solution.

15. SUBJECT TERMS Open, System, Technology, Information, Interoperability, IT, Collaboration, Networks, Cost, Financial, Microsoft, IBM, Google, Vulnerability, Hackers, Attacks, Evolution, GIG, Cyber, Cyberspace, Cyberwar, Legacy, Inventory, Acquisition, Competitive Advantage, Coalition Communications, Ubiquitous, Strategic, Centricity, Kaizen, ISO, Outsource

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	28	

USAWC STRATEGY RESEARCH PROJECT

DIVERSIFYING THE DEPARTMENT OF DEFENSE NETWORK ENTERPRISE WITH LINUX

by

Lieutenant Colonel Sherman LaCost
United States Army

Lieutenant Colonel Charles Grindle
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel Sherman LaCost

TITLE: Diversifying the Department of Defense Network Enterprise with Linux

FORMAT: Strategy Research Project

DATE: 14 March 2010 WORD COUNT: 5,850 PAGES: 28

KEY TERMS: Open, System, Technology, Information, Interoperability, IT, Collaboration, Networks, Cost, Financial, Microsoft, IBM, Google, Vulnerability, Hackers, Attacks, Evolution, GIG, Cyber, Cyberspace, Cyberwar, Legacy, Inventory, Acquisition, Competitive Advantage, Coalition Communications, Ubiquitous, Strategic, Centricity, Kaizen, ISO, Outsource

CLASSIFICATION: Unclassified

Historically, the United States and its closest allies have grown increasingly reliant on the technological evolution of automated systems. Those automated systems have provided continued efficiency, advancement and profitability to organizations around the globe. Despite the evolutionary advancements and corresponding economic strength associated with technological automation, the United States and its allies find themselves now globally tied to automation in a quest for daily existence. Due to our national reliance on these systems, the areas showing the most advancement also represent the greatest vulnerability if penetrated. Recognizing the strategic value to this global problem, this paper will set the stage to identify changes needed for our current client enterprise. The effective introduction of the Linux operating system at the client level will increase security, foster collaboration across all branches of government and decrease the fiscal tail of our current client-server solution.

DIVERSIFYING THE DEPARTMENT OF DEFENSE NETWORK ENTERPRISE WITH LINUX

Historically, the United States and its closest allies have grown increasingly reliant on the technological evolution of automated systems. Those automated systems have provided continued efficiency, advancement and profitability to organizations around the globe. Despite the evolutionary advancements and corresponding economic strength associated with technological automation, the United States and its allies find themselves now globally tied to automation in a quest for daily existence. Due to our national reliance on these systems, the areas showing the most advancement also represent the greatest vulnerability if penetrated. Recognizing the strategic value to this global problem, this paper will set the stage to identify changes needed for our current client enterprise. The effective introduction of the Linux operating system at the client level will increase security, foster collaboration across all branches of government and decrease the fiscal tail of our current client-server solution.

In recent years, many of our adversaries have modified their approach to attacking the United States and its allies by conducting networked attacks on infrastructure in an attempt to collect information on vulnerabilities and weaknesses. In the most recent years, attacks have originated from both foreign and domestic locations. Many attacks have been augmented by inadequate US policies regarding cyber warfare. Current U.S. cyber policy provides approaches abstaining U.S. forces from responding to attacks. Essentially the lack of response by our forces therefore encourages attackers to continue new penetration techniques.

The second order effect results in a grand stage for attackers to remain unchecked while continuing large scale global marketing through information operations. Unlike the traditional method of quantifying opponents by size, the virtual world allows non-state actors to easily maneuver and attack within traditional boundaries of large nations. This presents another series of complex issues related to dealing with non-traditional attacks from adversaries foreign and domestic.

Although this document must be tailored to one strategic area, the focus of this document will remain on the segment between the end user and first tier of their network. In this specific segment, the lack of diversity across the enterprise at the users desktop operating system represents a significant vulnerability. With the Microsoft Corporation (Microsoft©) providing the majority of systems occupying the Department of Defense (DoD) global enterprise, the potential for catastrophic failure across the enterprise when considering attackers prefer to conduct mass attacks tailored at Microsoft platforms[1].

During this assessment, there must first be a few bold assumptions to assist in setting boundaries for the quantification of the problem and the potential resolutions. As technology continues to develop at an increasing rate[2] it is important to understand changes in technology will continue to occur faster than a company's fiscal capacity to refresh hardware within traditional life cycle replacement programs. With the implementation of virtual technologies, administrators have found creative but technical constructs to migrate users from a thick client environment to virtual applications utilizing thin client techniques. The result has produced the capability to manage more assets and more users with fewer administrators.

It must be understood with limited physical and monetary resources in the coming years, the DoD will be required to provoke enterprise changes while adapting to changing techniques in cyber warfare and reducing fiscal investments. We must also acknowledge expected organizational behavior whereas individuals and organizations will respond with resistance to many of the new technologies and ideologic implementations. As Aristotle indicated in his research of the human response, the introduction of new ideas and technologies often create adversity and friction among users as well as their organizations[3]. Introductions of new concepts, technologies and creative configurations often evoke a series of intense network conflicts within and between domains to include global directories, new protocols, unique applications, network based devices and corresponding services.

We must also consider legacy systems will continue to exist as interoperability will remain a key concern while we continue to enforce standards and processes in our quest for global integration. Although changes in corporate and military networks will continue to occur, many of the countries within our coalitions may not upgrade software due to fiscal constraints or other factors. This lack of continuity across domains will represent additional challenges as legacy systems will inherently create unexpected second order effects impeding the operational and tactical levels of the global enterprise.

We must assume adversaries of the DoD to include dissident US residents will continue to attack our networks from foreign shores and domestic locations. We must assume adversaries who quietly collect information will eventually attempt to attack and/or deny the United States access to network based systems nationally or while

engaged in operations with its international partners. We must also assume many of the attempts will remain unchecked due to the continued reduction of administrators and technical staff through automation.

Both DoD and corporate networks will continue to find themselves under siege by applications and users alike. The DoD like many corporate companies have approved introducing applications into operational networks before substantial testing could be completed. The results were a series of unpredictable consequences impacting performance of our user base and negatively impacting the operational efficiency of both the networks and their supported organizations. Operationally, we must assume administrators will continue to provide accounts to users who find themselves introducing Virus's, Worms, Trojans and a series of other user preventable generated network events. As users remain creative in the way they bypass processes designed to protect the network, we must assume they will continue to remain a persistent challenge for administrators. We must also assume it is unlikely the current processes will keep the users from introducing unknown variants to operational networks without significant changes to the way networks are constructed and processes implemented.

In setting the readers expectations, this paper is not intended to evoke panic but instead encourage awareness and hearten change. The Microsoft Operating System has been maintained in the DoD inventory for more than 20 years. The competitive advantages in the future will require significant changes to our current inventory thereby opening doors to new technologies and facilitating new philosophies in our evolutionary development of command and control. It is also acknowledged the core competency of the DoD is not software development as the DoD would not utilize military members to

develop the initial load sets of any alternate solutions. It is expected the DoD would provide guidance and direction for assimilation of the requirements. The standard practice of outsourcing would remain the venue to produce products needed in implementation as the established acquisition programs would be sufficient to generate the desired effect.

When simplifying the role of vendor and customer (Microsoft and DoD), Microsoft's success and survivability is heavily dependent on its continued profitability and future capturing market share around the globe. As the corporation continues to grow, the need to attain more users across global locations assists in maintaining its sustained growth resulting in profits for shareholders. Changes in corporate strategy have effectively found new revenue streams through upgrades in software by discontinuing support to legacy platforms and forcing laggard consumers to upgrade. Each of these deliberate upgrades includes new pricing schemes designed to increase company revenue.

With the continued global growth of the Microsoft Corporation, it has been a standard business practice to release its core operating system overseas. Adding to the dilemma, Microsoft couples the overseas software release with other synergistic efforts as they provide code to develop new forms of hardware overseas. These necessary corporate strategies have allowed companies to spread overhead costs and sustain remarkable profit margins when times remain difficult for other organizations around the world.

Considering the strategic position in the defense of the DoD's infrastructure; the reliance on corporations to develop the majority of operating systems have essentially

outsourced our design, development and building of critical infrastructure to the very nations and nation states which we attempt to prevent from entry. Although the design of corporate strategy is to sustain profits, the protection of our nation is not Microsoft's top priority nor is it their core competency. The corporate sustainment of profitability has effectively neutralized the DoD's competitive advantage with other nations in the world of cyberspace. The worldwide release of sole proprietary products to other nations represents an exposure of exponentially unquantifiable proportion regarding the continued protection of DoD infrastructure.

In the competitive marketplace, strategy is defined as a firm’s theory on how it gains high levels of performance within its area of competency[4]. Although the continued growth of Microsoft provides strategic gains for itself and the overall economic gains in the U.S. economy; it represents a strategic exposure as the DoD cannot prevent penetration testing of its client operating system due to frequent worldwide releases at the corporate level. The Department of Defense for the United States represents only one of Microsoft's many large clients. Although many corporations often speak about how valuable their large customers are in the relationship management arena, the unfortunate fact is the DoD is just one of many clients Microsoft provides products worldwide.

The Microsoft Corporation's mission is to provide financial benefit to its shareholders, and sustained growth to its corporation[5]. Its focus remains on non state actors rather than the DoD’s focus of a nation state. The DoD remains focused on providing security to the nation[6] by remaining vigilant on issues concerning safety and security to the citizens of the United States. Since the early years of Microsoft's

development, the US Government utilized the products from Microsoft as a means to facilitate efficiency in operations while providing fair fiscal compensation to the Microsoft Corporation. What the DoD did not anticipate was the second order effect of a population utilizing this technological evolution and transforming into a population who became heavily dependent on technology along with other developing countries.

Evidence of the demand for technology can be seen in the global proliferation of the hand held wireless devices. The simple expansion of the cellular phone and other wireless devices has increased mobility and associated access to information. The networks providing access also serve as a venue for ill willed individuals to remotely penetrate the core population centers and utilize the access as a portal to exploit additional vulnerabilities.

Like all advances, increases in proficiency within the DoD began to assist the government in proliferating small networks and enabling better command and control. At the center of the client's desktop was the Windows® operating system. Although most people in today's economy focus on the need for unique or diverse individual applications rather than the operating system, the investments and lack of significant competition began to herd the majority of the US population toward a technological revolution and its dependency.

The resulting effect was a nation heavily reliant on the globalized economy. Today, standard family practices of on-line transactions are common. Utilizing on-line banking, bill payments, media distribution, on-line ordering of products, delivery of supplies, and a plethora of other services has become a staple for the US economy. As the population shifted more quickly than Microsoft could accommodate, competitors like

Linux and Apple have taken stronghold positions, filling the need in the user driven cyber marketplace.

Since Microsoft entered the market, it has remained aggressively positioned to occupy the majority of the marketplace by successfully capturing nearly ninety percent of today's market share[7]. Today Microsoft remains extensively populated in a multitude of industries including energy, financial services, transportation, communications, information services, and human services. Microsoft's long term strategy has been to get users "addicted[8]". The founder of Microsoft, Mr. William H. Gates, commented that Microsoft's success in the United States and around the globe will be very similar with how they roll out future copies of Windows to China as its latest developing enterprise. Mr. Gates was quoted; "As long as they are going to steal it, we want them to steal ours. They'll get sort of addicted, and then we'll somehow figure out how to collect sometime in the next decade"[9].

In the United States, Microsoft continues to creatively find ways to herd customers to newer versions of their software through discontinuation of legacy support. One might be led to believe users are provided "the opportunity" to purchase new versions as a way to evolve the masses. Microsoft like most large corporations is strongly encouraged to generate new revenue streams continuing their sustained economic growth. From a corporate perspective, a strong business model would suggest herding users into frequent upgrades resulting in continued waves of new revenue with lower operational overhead. This series of purchases would result in significant revenue from continuing sales and flush in new streams of cash to the company.

The dilemma is the sustainment of this need. Essentially, Microsoft needs to continue the practice of discontinuing support to legacy systems. Microsoft also needs to convey it was in the user's best interest to upgrade the operating system and repurchase third party software. Microsoft has become very successful at demonstrating this technique as indicated by their sustained double digit growth since their inception[10].

In the 2009 10K report[11] provided to stockholders, Microsoft acknowledged recent notable competitors in the market place threatening their long time monopolistic enterprise. Linux (a popular open systems platform) and Apple (a closed proprietary system) appear to be the most popular threats as larger corporations like IBM, NYSE, Ford Motor Corporation and Google Inc. have grown weary of the unconditional control and fiscal impacts Microsoft software represent to their product lines. In the past decade, large corporations have also demonstrated their ability to exercise alternate options in the event of an unexpected upgrade. Although not widely publicized, recent competitive advantages and resulting cost savings have demonstrated larger corporations are rethinking their software portfolio strategies. The result is a shift in the market on how large organizations are redistributing capital investments and recovering what was once regarded as sunk costs in software.

In an unprecedented enterprise wide decision, IBM executed an enterprise shift by replacing their entire Windows Server enterprise to a Linux solution. The move was prompted after Microsoft discontinued support to the Microsoft NT 4.0 platform. The Microsoft NT 4.0 platform was notably stable, provided stability for many years, very cost effective for customers, and very reliable. Microsoft's unconditional removal of support services for their platform strong armed the majority of companies around the

globe to upgrade to new software. Companies were left few options to prevent impeding their current operations[12].

The problem was felt in the government sector as the United States Army was also included in this strong arm approach[13]. The result for the U.S. Army was an unexpected thirty five million dollar service contract to Microsoft for six months of additional professional services while they attempted to scramble and prevent degradation of service to service members around the globe. Consequently the U.S. Army conceded to the six month contract along with a commitment to upgrade to new Microsoft software at an additional cost. The new fee structure was an unforeseeable consequence as the U.S. Government and other global organizations had no other choice but to upgrade or degrade operations.

IBM took note of this strong arm technique and conducted a cost benefit analysis on their options deciding to consider alternate routes. IBM found the cost savings in negated license fees allowed them to utilize the same projected costs to shift from Microsoft. In their solution, they implemented their own help desk who designed, implemented and supported their applications recompiled under the Linux operating system. The response to Microsoft sent a notable ripple across the worldwide corporate arena and subsequently caught Microsoft off guard. Shortly thereafter, Oracle followed suit after coming to the same conclusions along with Ford Motor Corporation[14] and several other companies.

After a few years, IBM moved Linux onto each of its employee’s desktop continuing to amplify the cost savings as well as providing better support to their users. The switch also augmented IBM's use of cost controls and predictable overhead to

efficiently customize applications to specific needs with increased security as well as enhance command and control. The implementation also provided an opportunity to lower the hardware requirements needed and increase processing capability as Linux is multi-threaded and not as memory or CPU demanding[15] as Microsoft operating systems.

IBM's success caused others in the marketplace to re-think the alternate solutions by driving the cost of ownership down by eliminating unnecessary business costs for its products. Consider Google's most recent introduction of "Android" software[16] which is projected to occupy over thirty percent of the market in hand held devices[17] by 2014. The Android software is also a Linux variant as its reduced cost and open systems design more easily interacts with mobile devices. The free cost of the Android software as compared to twenty five dollars cost per phone with Microsoft is also a market driver as companies look to squeeze overhead out of each product in difficult global markets.

The subsequent moves toward Linux also allowed companies to invest capital in more collaborative open system designs aligned with the open system standards. Microsoft has also had to rethink its position on dealing with companies who migrate to Linux by giving Linux credit on the Microsoft home page for Linux's interoperability with Microsoft Server products[18]. The change in strategy has subsequently also caused more companies to consider diversifying their networks with a combination of client server product not just pure Microsoft solutions.

At the strategic level across the current DoD enterprise, the global use of the Microsoft operating system remains extensive and lacks diversity at the user level. The

government has recently begun switching to technologies where the majority of users are running within virtual environments as to retain better command and control on the client service. While Microsoft provides a client with applications in the enterprise like outlook, web based, and office productivity suites, similar open source applications can be appropriated for open systems at substantially reduced cost[19]. Diverse open systems are also known for their interoperable capabilities[20] as well as notable survivability.

When considering a survivable and diverse open systems approach we still need to consider the desktop operating system. Single operating systems will present an increasingly large vulnerability. The world of networked devices continues to evolve smaller, lighter, more efficient solid state devices which require additional changes to their supporting operating systems. Provided the observation of Microsoft's evolutionary "bloatware" development[21], the shift toward other solutions remains a clear choice. The shift will continue to reduce the footprint as well as shifting toward mobility and flexible communications opportunities.

Other than the standard domain conflicts the DoD inventory is experiencing at the current time, increased diversity of operating systems will support the total force concept as well as reinforce the shift toward globalization in today's coalition friendly environment. As global partners and alliances remain on the forefront of today's conflicts, increased global integration and collaboration will be required in order to sustain the long war of tomorrow's battlefields. An open standards operating system will augment the long war by providing significant cost savings over the long haul when considering the cost to supply our coalition partners with ubiquitous inter-operable networked systems.

Reflecting on today's software portfolio it is important to note our coalition partners possess legacy software needed in their planning processes. When considering the DoD's software portfolio, International Organization for Standardization[22] (ISO) need to remain as a close reference guide when establishing requirements for future operating systems and subsequent application software. The continued government support of diversification could leverage corporate entities to establish industry standards thereby making software integration more inter-operable between vendors unlike many of the proprietary protocols and developments from several of today's large corporate product manufacturers. Although these trends from larger corporations are notable there are many other corporations setting ISO standards toward the benefit of the user population.

Today's market trends indicate network centricity continues to increase. With the downturn of the global economy hand held devices continue to be the top seller around the globe. Major companies like IBM, Google, Ford, Oracle, NYSE and a list others continue to demonstrate to the worldwide stage, open systems are appropriate to drive unnecessary costs out of the budget and free up needed capital for other investments. The U.S. Government needs to continue its network evolution while remaining light and agile to adapt to tomorrow's emerging threats. Diversifying with Linux at the client level will facilitate smaller less demanding devices. The shift will mobilize organizations and their communications around the world as devices continue to grow smaller with more integrated services.

The US Government also continues to invest heavily utilizing Small Business Innovation Research (SBIR) venues in an effort to maximize the human capital in

today's markets for new technologies. Small, large businesses, as well as institutions can anticipate government investments will continue for mobile technologies utilizing less expensive, open system standards. These strategic investments will facilitate the evolution of hardware and software portfolios. The continued investment strategy will open new opportunities and ideas from entrepreneurs supporting the United States.

As we focus on the strategic position of the DoD to deal with the current operating system dilemma, it is prudent to consider the diversification of the portfolio regarding DoD operating systems. Considering the successes of corporations in the civilian sector utilizing open system standards and dynamic infrastructure, the government can effectively demonstrate significant advancements in areas of cost avoidance, qualitative value associated with future technological advances, leveraging current SBIR advances, and technological competitive advantages.

Utilizing cost avoidance strategies, the US government can capitalize on cost savings from the negated volume license agreements with Microsoft. It can also begin to eliminate the yearly licenses renewed for third party software as the development teams can produce custom applications satisfying user requirements, in order to remain inter-operable and collaborative. As IBM initiated nearly ten years ago, the US government can redirect some of the cost savings to its own group of specialized engineers who develop and distribute the government version of collaborative but secure operating system. It is advisable to study lessons learned from larger corporations having implemented alternate solutions across their enterprise. The majority of the New York Stock Exchange (NYSE) trading systems utilize the Linux operating system. Through a series of custom applications designed to

compartmentalize, traders seamlessly execute multi-million dollar transactions each and every second within our most critical financial sectors of the United States.

At first glance, the suggestion of a variation of Linux is in line with the “best of breed” recommendations currently available. Large organizations like NYSE, IBM, Oracle, Conoco, Cisco, Google, Toyota, Ford, Panasonic, US Federal Courts, US Postal Service, Mexico City, State organizations, have all integrated large implementations of Linux into their infrastructure. The US Army is also utilizing Linux in its global AKO application as well as other areas. The recoupment or redirection of fees associated to licensing allows the government to develop its own help desk with personnel specializing in a more secure and user designed environment. The lack of distribution of the core operating system to adversarial foreign governments would represent a significant competitive advantage due to competing nation’s inability to actively test our product in a controlled environment. With the active integration of coalition forces around the world, the implementation is transparent to foreign countries. The “appearance” is perceived to allow unteathered access to our internal networks thereby facilitating more positive international diplomatic relations especially with the smaller nations. Reduction of the redundant platforms would also provide significant savings in hardware, software and corresponding licenses.

In its current configuration, if the government prefers to implement a change to the Microsoft operating system, the government needs concurrence from Microsoft who maintains all proprietary rights to the software. As Microsoft controls the majority of operating systems in the DoD inventory, the corporation has the right to deny the change of its proprietary software or charge significant fees associated to providing an

unsupportable software. In essence, the loss of controlling the core operating system provides additional obstacles to the DoD during a time when implementing new technologies is often difficult and time consuming at best.

In many cases, the government has had to obtain third party vendors to provide a work around to this barrier each time it occurs. This patch is often financially restraining, unsupported by the company controlling the operating system and ultimately has to be reworked as new versions of the operating system are introduced. With the proposed diversification, the government controlling the core operating system would decrease response times for implementations while decreasing the cost related Change Management errors. Additionally, the government will facilitate simultaneous enterprise changes into future upgrades.

The United States government also has access to the world's best and brightest with the utilization of the Small Business Innovation Research (SBIR) and Small Business Technology Transfer Program (STTR) programs[23]. The two programs have three focused groups: educational institutions, small business and highly skilled individual contributors. These groups bring creative solutions to government proposed problems. "The DoD SBIR program, funded at approximately $1.14 billion in FY 2008, is made up of 12 participating components… Army, Navy, Air Force, Missile Defense Agency (MDA), Defense Advanced Research Projects Agency (DARPA), Chemical Biological Defense (CBD), Special Operations Command (SOCOM), Defense Threat Reduction Agency (DTRA), National Geospatial-Intelligence Agency (NGA), Defense Logistics Agency (DLA), Defense Microelectronics Activity (DMEA), and the Office of Secretary of Defense (OSD).[24]" "The DoD STTR program, funded at approximately

$132 million in FY 2008, is made up of 6 participating components: Army, Navy, Air Force, Missile Defense Agency (MDA), Defense Advanced Research Projects Agency (DARPA), and the Office of Secretary of Defense (OSD).[25]" These programs have been in place for some time. The utilization of the programs can be augmented to bring new ideas and new technologies to fruition. Many of the programs already tout compatibility with Linux and other open systems. Future utilization of these pre-existing programs is beneficial to the DoD as the monies already invested and committed will further facilitate governmental goals toward interoperability and collaborative approaches.

Technological competitive advantage is the summation of value in all advantages. This sum includes the corresponding second order effects from the implemented changes. The U.S. has been losing it's competitive advantage as the corporation maintaining our current client regularly releases the system to our adversaries. The ability of foreign governments to test our core software in their own facilities represents a grave threat as they can openly test vulnerabilities for exploitation. With the Linux implementation, our government stands at an opportunity to advance command and control by preventing attackers the ability to conduct penetration testing in a controlled environment as they do now with the Microsoft product. As we utilize such programs as SBIR and STTR to bring new technologies to fruition and creative approaches to extremely complex problems, the United States Department of Defense also presented an opportunity to take its core operating system away from countries who test to exploit it. We also have an opportunity to change the conditions of the game unlike the leaders who have found themselves comfortable with a vulnerable Microsoft solution.

Ultimately diversity is a question of following our own moral compass. As the Rand Corporation[26] published for the United States Air Force, cyberspace attacks are difficult to defend and even more difficult to respond. Changing the game, controlling the environment, shaping the environment are the most creative and effective ways to strategically shape the environment setting attackers back for years or decades as they re-assimilate with new strategies. The focus of diversification is not to completely stop adversaries but to create imbalances and uncertainty in our enemy's plan of attack. Even at the most basic level of warfare, the introduction of diversity within our operating systems will add to the "fog of war" from our adversary's perspective.

Diversity is also a variable in risk mitigation. As we look to the future of implementing new technologies changing the way we conduct our core business; reviewing our portfolio of available products for users is more than just an attempt to distill down to one product in order to save costs. Risk mitigation suggests that although the start up costs may be higher in some regards, the long term run rate will be lower and the organization will be better. Diversification makes our networks stronger, more survivable, and resistive to unnecessary attacks from outside as well as inside our own firewalls. The change simplifies the user interface, interaction and removes the unnecessary bundled products distracting our users.

As major corporations increase diversity by switching to Linux and away from Microsoft, they demonstrate increasing resource pools existing within our marketplace effectively creating an environment to balance efficiency, proficiency and security. Corporations also demonstrate new ideas providing significant financial savings through cost avoidance and collaborative integration across the majority of platforms. Legacy

software systems currently in service within the DoD enterprise will be required to be repurchased due to Microsoft changing their operating system and focusing on a “goal of a clean installation of the operating system[27]” and eliminating the government’s opportunity to keep many viable and serviceable programs.

As the government ponders on the question, “why change our strategy and diversify?” The answer revolves around a few very simple concepts. In the current environment while in a wartime status, the government has had unprecedented lateral freedom in spending. As federal deficits continue to climb, the inevitable constriction of federal funding will occur. The cost avoidance model will allow curbing government spending while reinvesting capital savings into the network in forms of security upgrades, personnel and support infrastructure.

Governments continue to attempt to hold decision makers accountable for responsible fiscal decision making. As an example, the President of the United States recently called on Americans to remain vigilant and good stewards of U.S. Tax dollars[28]. Supported by other measures in previous administrations, the Sarbanes Oxley Act[29] was an attempt to place executive level processes in line with accountability for the private sector. The President continued to reinforce this again in his first State of the Union address as he recommended all entities government and civilian will again focus on ethical approaches when presented spending with limited or unlimited fiscal constraints.

While considering the Presidents direction of ethics, the question of investment strategy is brought to the forefront. As Google was recently subject to a large scale attack via a security flaw in their Microsoft Window's machines, it was again reinforced

to larger companies like Microsoft not to remain complacent about fixing issues. As an example, the Washington Post reported the details of a large scale attack on Google during January of 2010[30] where China exploited a backdoor in the Microsoft Operating system. Consequently Microsoft had known about the security flaw since September but had refused to place a fix until February which in this case was a month too late. Much like the Department of Defense, Google is also a very large corporation and customer of Microsoft. As indicated by the lack of timely action by Microsoft, the size and the need of the organization does not guarantee a fix from corporations who assess a risk to their customers networks.

As the United States stands at the forefront of impending budgetary action[31], Congress will undoubtedly take drastic action in an attempt to curb spending across all lines to reduce the federal deficit. Despite the President's call for limitations on where cuts can or cannot occur, decision makers are reminded the budget is approved and executed by the United States Congress and not the President of the United States[32]. Adding to the bureaucratic dilemma is the question of transparency for programs utilizing tax payer dollars to support its infrastructure. Cost saving programs will remain extremely important in positioning efforts for those who will require federal funds in the coming years.

As government officials continue to make strategically targeted areas for improvement within our infrastructure, the decision makers must reinforce and strengthen our networks through measures of enhanced interoperability. Fiscal decisions will benefit positively while augmenting risk mitigation practices through the balancing of information technology portfolios. Client operating systems such as Linux

will continue to diversify these portfolios thereby adding strength both qualitatively and quantitatively. The choice remains an ethical decision where on one hand the United States could stay on the current path by "kicking the can down the road[33]" or decide to make a fiscally prudent and morally sound choice for the long term support of our infrastructure. Its implementation fosters an environment of better command and control through the use of continuous improvement processes (Kaizen)[34]. In choosing the Linux client operating system, the move encourages open standards, reduces the governments total cost of ownership, increases interoperability, removes the unnecessary exportation of our core operating systems, and encourages standards keeping large and small businesses competitive. Finally, installing Linux at the client level across the enterprise will most importantly assist the United States by encouraging competitive markets to develop heterogeneous technologies ushering in tomorrow's technologies to a world supporting ubiquitous collaboration at all levels of government while simultaneously working hand in hand on supporting the relationship development of our coalition partners.

Endnotes

[1] *Google Hack Attack Was Ultra Sophisticated*, http://www.wired.com/threatlevel/2010/01/operation-aurora (accessed February 21, 2010)

[2] *IEEE Moore's Law*, http://sscs.org/History/MooresLaw.htm (accessed January 24, 2010)

[3] *Aristotle's Seven Causes of Human Action*, http://www.huomah.com/Conversions/Conversion-Strategies/Aristotles-7-Causes-of-Human-Actions.html (accessed February 6, 2010)

[4] Jay B. Barney, *Gaining and Sustaining Competitive Advantage* (Upper Saddle River, NJ: Pearson Prentice Hall, 2007), 4.

[5] *Microsoft Corporation Home Page*, http://www.microsoft.com (accessed January 24, 2010)

[6] *Department of Defense Home Page*, http://www.defense.gov/admin/about.html (accessed January 24, 2010)

[7] *CIO Magazine* http://www.cio.com/article/467916/Microsoft_Market_Share_Slips_Pressure_s_On_for_Windows_7_and_IE8 (accessed January 24, 2010)

[8] *Linux Magazine* http://www.linux-mag.com/cache/7669/1.html" (accessed January 24, 2010)

[9] Ibid

[10] *Microsoft Corporation Investor Relations* http://www.microsoft.com/msft/reports/ar08/10k_dl_dow.html (Accessed January 24, 2010)

[11] Ibid

[12] *Microsoft winds down Windows NT sales,* http://news.cnet.com/2100-1001-273847.html (accessed February 6, 2010)

[13] *Army Extends Windows NT 4.0 Life Support; VARs Pay The Price,* http://www.crn.com/government/57300633;jsessionid=FDKTTIODMCMZJQE1GHRSKH4ATMY32JVN (accessed February 6, 2010)

[14] *The Register*, http://www.theregister.co.uk/2003/09/15/motor_giant_ford_to_move/ (accessed January 24, 2010)

[15] *Bellevue Linux Group*, http://www.bellevuelinux.org/reasons_to_convert.html (accessed January 24, 2010)

[16] *Jessica* E. Vascellaro "*Google Wagers on Cellphone Ads*" Wall Street Journal, Nov 10, 2009:B.1

[17] Saul *Hansell* "Big Cellphone Makers Shifting to Android System" New York Times, Oct 26, 2009: B.4

[18] *Compare Windows to Linux*, http://www.microsoft.com/windowsserver/compare/linux/windows-server-interoperability.mspx (accessed February 6, 2010)

[19] *Openoffice.org review*, http://www.pcmag.com/article2/0,2817,1848660,00.asp (accessed February 7, 2010)

[20] *LETSI: The International Federation for Learning, Education, and Training Systems Interoperability,* https://letsi.org/ (accessed February 7, 2010)

[21] *Microsoft's bloatware problem*, http://news.cnet.com/8301-13505_3-9729642-16.html (accessed February 21, 2010)

[22] *International Organization for Standardization*, http://www.iso.org/iso/home.htm (accessed January 24, 2010)

[23] *Small Business Innovation Research*, "http://www.acq.osd.mil/osbp/sbir/overview/index.htm" (accessed December 15, 2009)

[24] Ibid

[25] Ibid

[26] RAND Annual Report 2009, http://www.rand.org/pubs/annual_reports/AR7145/ (accessed January 5, 2010

[27] *The Windows 7 Ecosystem*, http://news.softpedia.com/news/The-Windows-7-Ecosystem-93853.shtml (accessed February 6, 2010)

[28] *Remarks by the President before Signing the Tax Delinquency Memorandum*, http://www.docstoc.com/docs/23116900/Remarks-by-the-President-before-Signing-the-Tax-Delinquency-Memorandum (accessed February 6, 2010)

[29] *The Sarbanes Oxley Act*, http://www.soxlaw.com/index.htm (accessed February 4, 2010)

[30] *Google attack highlights 'zero-day' black market,* http://www.washingtonpost.com/wp-dyn/content/article/2010/01/29/AR2010012902017.html (accessed February 5, 2010)

[31] *Obama to seek spending freeze to trim deficit*, http://www.nytimes.com/2010/01/26/us/politics/26budget.html (assessed January 25, 2010)

[32] *The Office of Management and Budget*, http://www.whitehouse.gov/omb/ (accessed February 6, 2010)

[33] *Budget fixes are simple – and unthinkable*, http://www.cnn.com/2010/OPINION/02/04/zakaria.budget.deficit/index.html?iref=allsearch (accessed February 6, 2010)

[34] *How Toyota and Linux Keep Collaboration Simple*, http://hbswk.hbs.edu/archive/4928.html (accessed February 6, 2010)