Analysis of Cyber Security Methodologies: A Direct Comparison of Current Versus Possible DoD Cyber Assets

Sai Kumar and Vikram Mittal

Department of Systems Engineering
United States Military Academy
West Point, NY 10996, USA

Corresponding author's Email: vikram.mittal@westpoint.edu

Author Note: Sai Kumar is a cadet at the United States Military Academy and is a Systems Engineering Major. Dr. Vikram Mittal is an assistant professor at the United States Military Academy within the Systems Engineering Department and is the advisor for this honors thesis. Sai Kumar would like to thank all of the personnel and stakeholders that contributed their time towards informing this paper and Dr. Mittal for all the time he has spent helping to connect the dots in this paper.

Abstract: Recent years and modern warfare have shown an increasing reliance on the cyber domain to maintain national and military operability, resulting in cyber exploits having a more profound impact on victim nations. As the United States seeks to maximize its ability to capitalize on these exploits and minimize its susceptibility, a decision must be made on the most effective way to accomplish these tasks. Currently, each major department within the Department of Defense (DoD) are methodically building up their own cyber assets to accomplish these tasks as they relate to their traditional domain. There has been a recent proposal to do away with this system structure and instead create a separate Cyber Department, on the same level as the Army, Navy, etc. This paper evaluates the comparative value between the two proposals through value modeling. The value model is based on each alternative's ability to achieve the end state cyber goals of the DoD and the nation as a whole. Strong indicators point towards a separate Cyber Department as the most valuable alternative available to achieve the nation's goals, and that there are current weaknesses within our current cyber structure that are open for exploitation.

Keywords: Cyber , Cyber Security, Department of Defense Reorganization, National Security, Cyber Department, Cyber Command Structure, Cyber Domain, Cyber Assets, Modern Warfare

1. Introduction

The aim of the Department of Defense (DoD) is to ensure the survival of the United States via the accumulation and training of the necessary resources that guarantee its ability to protect the United States. This protection can take many forms from both defensive tactics to offensive movements that ensure the future security of the nation. Immediate defensive strategies focus on the countering and mitigation of vulnerabilities in the securing of national assets, while offensive strategies are focused on exploiting these weaknesses in opposing nations. During recent years, the emergent cyber domain has highlighted both current weaknesses in and future opportunities for the DoD. In recent years, the utilization of cyber assets to assist in the conventional methods of warfare has increasingly risen to prominence, both domestically and abroad. Notably, the Stuxnet virus brought to bear the overarching capabilities and reach that cyber weapons hold (Langner, 2011).

The conventional sense of cyber warfare tends to be associated solely with digital implications such as information compromise, blocking information and signal reception, and/or the shutdown of electronic assets. However, cyber warfare is very much capable of causing physical damage, and the Stuxnet attack of 2009 proved just that. Stuxnet targeted the industrial controllers of Iranian nuclear facilities through malware that was specifically designed for controllers manufactured by Siemens (Langner, 2011). After gaining access to the controller and verifying that it was the correct target type, Stuxnet then caused valves on centrifuges in the nuclear facilities to increase the pressure within them to the point that they broke (Zetter, 2014). For the first time the world was truly exposed to the type and scale of damage that cyber warfare is capable of, and ever since the Stuxnet attack, countries around the world have been in competition to build cyber assets to capitalize on these capabilities.

The growing cyber capabilities of near-peer nations has been on display in the past couple of years. In 2016, Ukraine experienced a cyber-attack that operated on an unprecedented scale in terms of precision and number of users affected. Russia has denied culpability but is both accused by Ukraine as the culprit, as well as is pegged by leading cybersecurity analysts as the main suspect (Greenberg, 2017). These cyber-attacks once again highlighted the ability for cyber warfare to cross over from the virtual to physical realm by effectively shutting down all electrical infrastructure for approximately 225,000 customers (Lee, Assante & Conway, 2016). However, Ukraine was able to return services promptly due to their retention of manual override controls. Conversely, in the United States infrastructure system manual override controls are no longer present in control systems, and the security of these control systems are arguably worse than that of Ukraine; which indicates that a sophisticated blackout attack, like the one Ukraine suffered, could last much longer than a couple hours, in the range of weeks to months. Furthermore, recent analysis conducted by experts in this field concluded that the United States is only realistically prepared to survive a week of power outage before there is absolute chaos (Koppel, 2015). This means that the value of preventing cyberattacks is not in the scale of thousands or millions, but, with total losses combined, approaches the scale of billions and possibly even trillions, depending on the length of duration (Amadeo, 2018).

These incidents highlight the massive damage that cyber-attacks are capable of, as well as emphasize the importance of the DoD's method to both develop these weapons and prevent their use on US systems. Furthermore, the ability to grow offensive capabilities is just as vital to the DoD in terms of furthering military dominance, because these offensive capabilities exponentially increase the striking range of the DoD. In comparison to conventional warfare, where troops had to physically seize control of key military assets, offensive cyber capabilities open up the possibility of achieving this remotely. The DoD's current policy for addressing this emergent field is the development of individual cyber branches within each Service. However, a recent proposal suggested creating a unique department within the DoD to solely focus on this domain (Stavridis & Weinstein, 2014). The purpose of this paper will be to identify weaknesses within current cyber integration methods and then determine if a unique Cyber Department would improve, maintain, or exacerbate these problems. The current cyber structure will be evaluated quantitatively, while the proposed Cyber Department will be analyzed partially quantitatively and partially qualitatively due to limited data.

2. Underlying Assumptions

To analyze the current DoD system with that of an independent branch, some underlying assumptions must be made. First, the analysis will be based on five main value measures: integration with conventional forces, resource utilization, response time, effectiveness, and the ability to build future weapons. Each of these measures contain unique reasons for their importance that are derived from the Army Cyber Command Mission Statement ("U.S. Army Cyber Command | The U.S. Army", 2018). The decomposition of these measures is shown in the value hierarchy in Figure 1. Secondly, since there is not a fully simulated version of what the actual DoD proposal for a separate Cyber Department would resemble, the values for a separate Cyber Department will be mainly based off how current DoD departments are structured and interact with each other. Third, each of the values will be benchmarked in 25-point intervals due to the limited information concerning the exact interactions between differences in values and department performance.

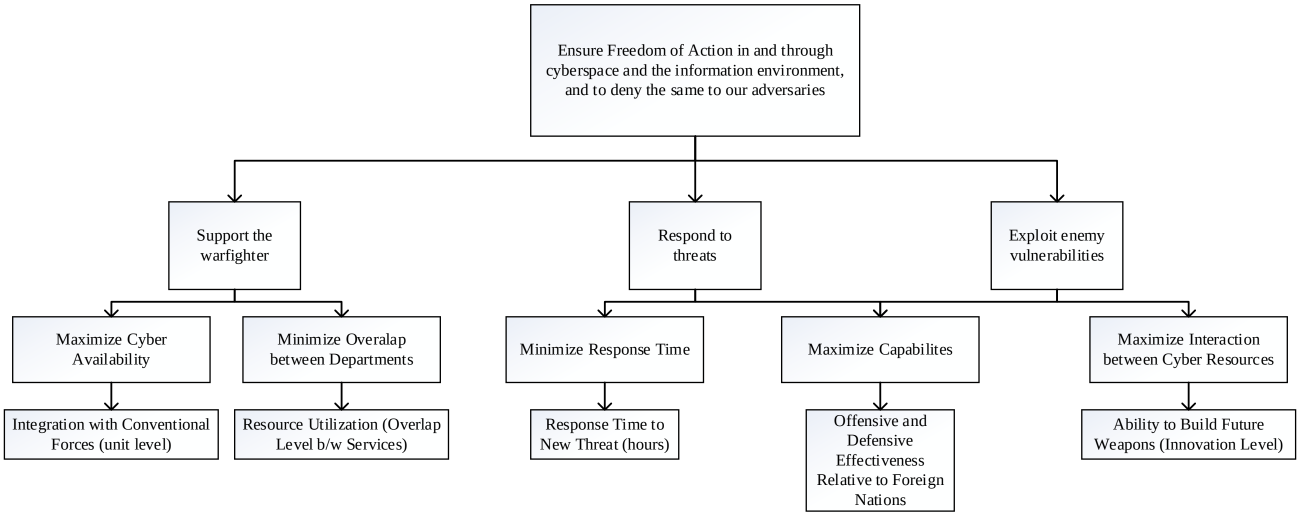
Ensure Freedom of Action in and through cyberspace and the information environment, and to deny the same to our adversaries
Support the warfighter
Respond to threats
Exploit enemy vulnerabilities
Maximize Cyber Availability
Minimize Overalap between Departments
Minimize Response Time
Maximize Capabilites
Maximize Interaction between Cyber Resources
Integration with Conventional Forces (unit level)
Resource Utilization (Overlap Level b/w Services)
Response Time to New Threat (hours)
Offensive and Defensive Effectiveness Relative to Foreign Nations
Ability to Build Future Weapons (Innovation Level)

Figure 1: Value Hierarchy of DoD Cyber Assets

Precise performance data and the resulting distributions are assessed internally and not made public. However, since the general correlations between these values and system performance are known, it is a reasonable assumption to break down these values similarly and with incremental jumps between value assignments. The generation of these value measurements and scores are shown below in Figure 1 and Table 1, respectively.

Table 1. Value Scale of DoD Cyber Assets

Value Measure	0	25	50	75	100
Integration	Cyber utilization at the strategic level	Cyber utilization at the division level	Cyber utilization at the brigade level	Cyber utilization at the battalion level	Cyber utilization at the platoon level
Resource Maximization	Similar resources with a similar mission set being represented in every DoD department	Similar resources in every DoD department with slightly different mission sets	Similar cyber resources in every DoD department, but unique mission sets	Related cyber resources in every DoD department and unique mission sets	No repetition of similar resources with a similar mission in any DoD department
Flexibility	>72 hours to deploy assets	24-72 hours to deploy assets	12-24 hours to deploy assets	2-12 hours to deploy assets	<2 hours to deploy assets
Effectiveness	Ineffective offensive and defensive cyber Domains	One ineffective domain, one moderately effective domain	One extremely effective domain, one ineffective domain/ two moderate domains	One extremely effective domain, one moderate domain	Extremely effective offensive and defensive capabilities
Ability to Build Future Weapons	No innovative overlap between cyber assets	Slight overlap between cyber assets	Intermediate overlap between cyber assets	High levels of overlap and communication between cyber assets	Complete overlap of cyber research and circulation of research and innovation between all cyber assets

The first value measure, integration with conventional forces, is defined by the operational unit level that is able to utilize cyber resources. The ability to integrate is a critical test in modern warfare due to the necessity of integration for cyber forces to successfully support and increase the effectiveness of conventional forces (U.S. Army Cyber Command, 2016). Without tight integration with conventional forces, limitations are imposed on the precision of cyber-attacks due to the confines of attacks based off of strategic level information. However, when cyber forces are tightly integrated with conventional forces, the latter can call in precise target locations and desired assets (i.e. drone reconnaissance, drone attacks, denial of service attacks on specific servers, etc.) at the forward deployed level, thereby maximizing mutual benefits. This would optimize both the conventional forces ability to eliminate threats through targeted takedowns of key enemy assets as well as optimize the tactical aspect of cyber forces' support of the mission. Integration will be one of the most important values assessed because of its necessity for meeting the requirements of modern warfare, where smaller and smaller units are predicted to operate independently (Barno & Bensahel, 2017). The scale for integration, as well as the other value measures, are displayed above in Table 1.

Resource utilization is a key component of testing system effectiveness, due to the environment in which national cyber forces will be funded and developed. Both options currently being discussed for cyber forces are government assets that will be funded by taxes. As a result, it is the duty of the government to ensure that taxpayers' funds are being used to develop the most resource optimal solution possible and to minimize expenditures. Resource utilization is defined as the elimination of redundant resources being utilized for similar purposes throughout the DoD. Resource utilization is an incredibly important value measure due to the recent debates over military budgeting. Therefore showing the taxpayers that they are getting the absolute most for their money is critical to ensuring the successful resourcing of the DoD as a whole (McCarthy, 2018).

Response time is another vital aspect to determining system effectiveness due to the nature of war, especially in the cyber domain. Entire wars have been characterized by moments of action, and in the cyber realm this is fast forwarded to an unprecedented level. Cyberattacks can occur without notice and leave only a limited window of opportunity open for a counterattack that mitigates impact. Furthermore, the damage that cyberattacks cause exponentially increases the longer the response time is delayed. ("Cyber Incident Response: What Is It, And Why Do You Need It? - Securonix", 2017). Response time is defined as how quickly the command structure is able to deploy a significant level of assets (i.e. traditionally a company sized unit or higher) on an immediate threat, opportunity, or respond to an attack. Response time is relatively important due to the necessity for quick responses to the ever present threat level of the post-Cold War world (Hermes, 2001). The scale for response time is displayed in Table 1 and is capped at 72 hours due to the correlation between response time and containment time (Kilcarr, 2016). The corresponding times between response and containment indicate that past 72 hours would push full containment over the week estimate for the United States ability to avoid chaos.

Effectiveness is critical to system performance due to the inherent nature of required effectiveness for system functionality. Effectiveness will be a combination of the qualitative measurements of cyber capabilities in the offensive and defensive domain. Ultimately, effectiveness is the most important value that will be measured, because this is the ultimate determination of what command structure will best facilitate the mission of the DoD, which is to protect and defend the American people and way of life (Department of Defense, 2018).

Finally, for a domain with the rapid innovation rate that cyber has where new technology possible becomes obsolete within a couple weeks and not years, the ability to build future weapons both efficiently and rapidly is critical to the capability of the United States to maintain its lead in military lethality. The ability to build future weapons is defined as the amount of innovation fostered by the command structure, because innovation is the defining feature of new product development. Ability to build future weapons is the lowest weighted value due to two factors: the prevailing necessity to focus on current cyber issues before those of the future and the inability to accurately predict what drives innovation. Fortune 500 Companies spend hundreds of millions of dollar trying to foster innovation without achieving a finite definition as to what drives innovation. Innovation can spring from any source in any place due to the unpredictability of the human mind, however there are certain rules that, in general, help to foster a more innovative environment, such as grouping similar projects/engineers next to each other, encouraging the sharing of information between likeminded personnel, etc. (Albury, 2005).

The one major value that will not be assessed in this paper is that of cost. There are a few limitations and assumptions that necessitate this step in building an accurate model. The first of which is the lack of accurate data on the cost of a Cyber Department capable of dealing with national defense and offense tactics. In just the past decade alone, the importance of cyber has grown at an exponential and unpredictable rate, which is why scaling is such an important aspect of the response time value (Choucri, Madnick & Ferwerda, 2013). Furthermore, the nature of the domain means that large breakthroughs will continue to create nearly instantaneous effects, which makes the future growth rates necessary to meet demand nearly impossible to accurately predict. Without more predictable growth rates, a fully costed price tag for the system is unreliable as well. Second, in the current structure there is no truly reliable source of cost data. The Army Cyber Department is a little over four years old and is very much in the building phase. Publicly available cost data for a classified department is still many years away. Finally, the major assumption that allows for the negating of these limitations is the exponentially rising cost of potential cyber-attacks, calculated in both monetary value to repair damages as well as the opportunity cost of having critical systems shut down for an extended period of time, makes the cost of any significant improvement in cyber capabilities a dominating option. This assumption is reasonably backed up by the high fines imposed daily on US infrastructure systems that do not comply with national cyber guidelines, due to this very reason (Sullivan & Kamensky, 2017).

3. Results and Analysis

These criteria were evaluated through a value model that used outside sources to assess value levels for each alternative and assign weights based on the relative importance of the value, briefly discussed above. The resulting model outputs are displayed below [Table 2 and Figure 2]. Notably, the separate Cyber Department alternative was evaluated through both the historical analogy for the creation of the Air Force as well as extrapolation of current system readiness levels in current DoD Departments, since there is very little data on an actual Cyber Department.

For integration, the current cyber structure received a 25 because of the current process by which Army Cyber officers are being integrated into the force. Currently upon completion of their Basic Officer Leadership Course where they are taught how to be cyber officers, they can post to certain command elements where there are National Security Agency (NSA) outposts. This indicates that Army Cyber officers are being grouped at the division level since they are post specific and are not fully integrated into lower level units. For resource utilization, the current cyber structure was assigned a 25 due to the current buildup of similar assets in every DoD department with slightly different mission sets. The main difference in their mission sets stems from their dedication to supporting their specific branch, and not an actual difference in domain-specific goals. This is exemplified in the same specifications being used to determine cyber readiness across the different services (Pomerleau, 2017a). The current cyber structure scored a 50 on response time due to the scale of time it would take to deploy a company-sized element. Under the current system, quick reaction force companies have been developed within the Army that would facilitate a deployment of within 24 hours (Cox, 2018). The current cyber structure score a 25 on effectiveness due to the current ineffectiveness in creating a holistic, national cyber defense while maintaining a moderate offensive effectiveness level. This can be seen in the far ranging limitations in current US cyber networks that would leave it open to an attack similar to the one demonstrated in Ukraine (Greenberg, 2017). Whereas in the offensive realm, the US has shown moderate capabilities to deploy cyber-attacks, as seen in Stuxnet. However, US Military Forces have been unable to fully leverage the cyber domain in current wars in Iraq and Afghanistan, via the domination of the cyber domain to amplify units' warfighting capabilities (Commons, 2018). The combination of these factors leads to a rating of moderate for offensive capabilities.

A separate Cyber Department was assigned a value of 75 for integration because of the current integration level of combined arms warfare within the DoD. Due to recent counter insurgency operations in Iraq and Afghanistan, the capability for the DoD to conduct combined arms warfare has dropped from pre-Global War on Terror levels. This is due to the necessity for counterinsurgency operations to focus on the protection of the civilian population, which has led to isolated units focusing on their area and to work at smaller unit levels that can better interact with the populace. The result of this lower unit level focus is that the DoD's ability to conduct combined arms warfare has dropped due to the limited necessity and training between units and departments to mass their destructive effects. However, the current capability within the DoD to conduct combined arms warfare between Departments is still assessed to be at the battalion commander level and still notably higher than the current cyber structure (Richardson, 2012). The assumption as to why separate departments would have a higher integration level than units within the department itself comes down to resource allocation. Right now cyber officers are too sparse in the Army to effectively integrate at levels lower than the division due to the essential ownership of assets by command levels, which leads to the issue where commanders are reluctant to relinquish control of assets assigned to them. However, a Cyber Department could pool personnel and then transition from Department to Department as needed when in the area of operation.

The Cyber Department was assigned a value of 75 for resource utilization because of the past precedent of the transformation of the Army Air Corps into a separate entity known as the Air Force. While the Air Force took the majority of air assets, each department created air assets with unique technological factors that made them essential to their mission accomplishment. This is highlighted in the specialization of the Army in helicopters in order to facilitate troop movements through vertical takeoffs and the specialization of the Navy in carrier-equipped jets in order to facilitate overhead firepower in naval battles ("Army Air Forces - United States Army Aviation", 2018). Therefore, it is assumed that the creation of a Cyber Department would follow the same path, whereby the majority of cyber assets and mission sets that overlapped between the departments would be consumed by the new Cyber Department while each department would develop cyber assets that are actually critical and unique to their individual mission sets.

The Cyber Department was assigned a value of 50 for response time due to the presumption that current mobilization rates would most likely not change with the creation of a new department. Since in the event of a mass mobilization scenario, each department secretary would be tasked with mobilization under the same time constraints, there would be no noticeable difference in the mobilization rates due to similar mobilization requirements. The effectiveness of a separate Cyber Department was ranked at 75 because of the comparable ratio in effectiveness that the Air Force underwent after their separation from the Army. After the separation, the Air Force suddenly became an equal to the Army both in the political realm and in importance of funding, which lead to a considerable increase in air power technology and airmen (Hammons, 2016). Paralleling this, the same could be expected to come true of a separate Cyber Department.

The ability to build future weapons of a separate Cyber Department was valued at 75 due to the increased level of overlap that would result from a separate entity dedicated to cyber operations. The current cyber structure has assets scattered across three departments, where the natural barriers between departments hinder cooperation and innovation. A separate Cyber Department would partially remove these barriers by grouping all resources dedicated to cyber research and weapon creation in the same department and would most likely encourage the circulation of cyber related information, thereby fostering innovation (Albury, 2005). Realistically though there seems to be no cyber structure within the DoD that would achieve a score of 100 on the ability to build future weapons, since the necessity of a classification system hinders the possibility of unexpected innovators offering up their solution. However, a separate Cyber Department would go a long way towards maximizing the DoD's ability to foster innovative solutions.

Due to the results of this research, it is recommended that the DoD further investigate and pursue the alternative to establish a separate Cyber Department. The benefits of separating domains into their own departments is evident in the historical example of the US Air Force. The US Air Force now dominates the world as a leader in air power technology and the same could be true of US cyber forces if a similar approach was taken (Attar, 2017). Without these added benefits of a Department dedicated to the emergent cyber domain, the US risks potentially losing the military edge it has maintained in the modern era.

Table 2. Value Model Scores of Cyber Structures

Value Measure	Global Weight	Unweighted Score		Weighted Score	
		Current Cyber Structure	Separate Cyber Branch	Current Cyber Structure	Separate Cyber Branch
Integration	0.20	25	75	5.0	15.0
Resource Maximization	0.22	25	75	5.5	16.5
Flexibility	0.15	50	50	7.5	7.5
Effectiveness	0.30	25	75	7.5	22.5
Ability to Build Future Weapons	0.13	25	75	3.3	9.8
Total Value Score	1.00			**28.8**	**71.3**

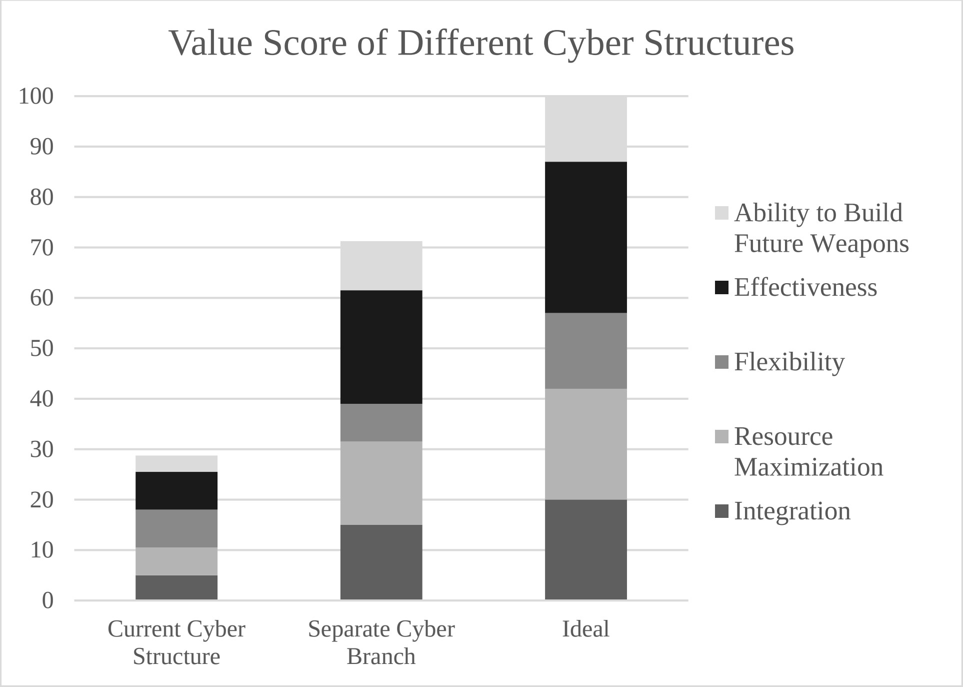

Figure 2. Value Model Scores Graph of Cyber Structures

4. Discussion and Future Work

This analysis used primarily constructed scales tied to the inherent military cyber functions. The use of constructed scales are somewhat limiting in that they rely on interpretation of the current state of each alternative based on available information. However, the results still show that with the current understanding of the cyber domain's importance and pace of innovation, a separate Cyber Department would prove to be the alternative best suited to achieve national goals. However, there are modifications that would strengthen the results of this research. First, access to higher levels of data concerning cyber structures and mission sets would increase the level of accuracy in the assignment of value measures. Furthermore, a higher level of data access would facilitate the implementation of the cost aspect of this model, due to the ability to review the classified documents surrounding the costing and structure of the current cyber structure as well as for the current DoD Departments. Finally, a confounding element of this research is a lack of clear and unifying mission set for the DoD cyber resources. Currently, most mission sets pushed down from the national level are vague and do not have tangible measurements. This is to be expected because of the ambiguity concerning exactly how the cyber domain will affect military operations as well as the current dilemma of confounding roles between the NSA and DoD Cyber Command. However, as this understanding and distinction begins to solidify in the future it is a necessity that hard and clear objectives begin to be issued (Pomerleau, 2017b). This would lead into the reevaluation and recalibration of this model according to the objectives defined by national statements and not just the objectives that are generally recommended for overarching cyber assets, both foreign and domestic.

5. Conclusion

The rising emergence of the cyber domain has shaken common understandings of how the military operates. A largely doctrinal and slow-moving organization is being forced to adapt its procedures at an unprecedented pace. This unprecedented pace is most notable in the comparison of timelines for the last major DoD department creation. The Army Air Corps was in operation for nearly thirty years before being spiraled off into the Air Force (Hammons, 2016). Whereas, the Army Cyber Branch has been in existence for a little over four years and there is already serious consideration of creating a separate department ("Timeline of Army Cyber", 2017). This does not reflect poorly on the ability of the Army, or other DoD departments, to fulfill cyber obligations, but is instead a reflection on the immense importance that the cyber domain holds in modern warfare. This paper has taken a step in the right direction for determining the cyber needs of the US Military by highlighting how a separate Cyber Department could propel our national defense industry forward in this new domain. However, much more needs to be done to ensure that if DoD decides to pursue a separate Cyber Department, it is implemented in a way that maximizes its impact. The ramifications of not doing so are already becoming apparent in global examples.

6. Acknowledgments

This paper was previously published and presented in the Donald R. Keith Memorial Capstone Conference at USMA in May of 2018. Any opinions, findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the United States Military Academy, United States Army, or United States Department of Defense.

7. References

Albury, D. (2005). Fostering Innovation in Public Services. *Public Money And Management*, *25*(1), 51-56.

Amadeo, K. (2018). *5 U.S. GDP Statistics You Need to Know*. *The Balance*. Retrieved 8 March 2018, from https://www.thebalance.com/u-s-gdp-5-latest-statistics-and-how-to-use-them-3306041

Army Air Forces - United States Army Aviation. (2018). *Army.mil*. Retrieved 8 March 2018, from https://www.army.mil/aviation/airforces/index.html

Attar, A. (2017). *10 Highly Powerful Air Forces in the World (2018 Ranking)*. *ListoGraphic*. Retrieved 8 March 2018, from http://listographic.com/10-powerful-air-force

Barno, D., & Bensahel, N. (2017). *Three Things the Army Chief of Staff Wants You to Know*. *War on the Rocks*. Retrieved 8 March 2018, from https://warontherocks.com/2017/05/three-things-the-army-chief-of-staff-wants-you-to-know/

Choucri, N., Madnick, S., & Ferwerda, J. (2013). Institutions for Cyber Security: International Responses and Global Imperatives. *Information Technology For Development*, *20*(2), 96-121. http://dx.doi.org/10.1080/02681102.2013.836699

Commons, A. (2018). Cyber is the New Air Domain Superiority in the Megacity. *Military Review*. Retrieved from http://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2018/cyber-is-the-New-Air-Domain-Superiority-in-the-Megacity/

Cox, M. (2018). *Army to Stress More Emergency-Deployment Training in 2018*. *Military.com*. Retrieved 8 March 2018, from https://www.military.com/daily-news/2018/02/13/army-stress-more-emergency-deployment-training-2018.html

Cyber Incident Response: What Is It, And Why Do You Need It? - Securonix. (2017). *Securonix*. Retrieved 25 March 2018, from https://www.securonix.com/cyber-incident-response/

Department of Defense. (2018). *Summary of the National Defense Strategy of The United States of America* (p. 1). United States of America.

Greenberg, A. (2017). *How An Entire Nation Became Russia's Test Lab for Cyberwar*. *WIRED*. Retrieved 8 March 2018, from https://www.wired.com/story/russian-hackers-attack-ukraine/

Hammons, M. (2016). *The Origin of the U.S. Air Force - VeteranAid*. *VeteranAid*. Retrieved 8 March 2018, from https://www.veteranaid.org/blog/2016/04/12/the-origin-of-the-u-s-air-force/

Hermes, W. (2001). *American Military History* (pp. 591-619). United States Army. Retrieved from https://history.army.mil/books/AMH/AMH-27.htm

Kilcarr, S. (2016). *Survey says corporate cyber response still too slow*. *Fleet Owner*. Retrieved 25 March 2018, from http://www.fleetowner.com/blog/survey-says-corporate-cyber-response-still-too-slow

Koppel, T. (2015). *Lights out* (pp. 121-126). New York: Broadway Books.

Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy Magazine*, *9*(3), 49-51. http://dx.doi.org/10.1109/msp.2011.67

Lee, R., Assante, M., & Conway, T. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. *Electricity Information Sharing And Analysis Center*, v-vi. Retrieved from https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

McCarthy, T. (2018). *Does the US really need a huge boost in military spending?*. *The Guardian*. Retrieved 8 March 2018, from https://www.theguardian.com/us-news/2018/feb/09/senate-budget-deal-us-military-spending

Pomerleau, M. (2017a). *Army, Navy Cyber teams say they're ready to go ... a year early*. *Fifth Domain*. Retrieved 8 March 2018, from https://www.fifthdomain.com/dod/2017/11/02/army-navy-cyber-teams-say-theyre-ready-to-go-a-year-early/

Pomerleau, M. (2017b). *DoD still working toward CYBERCOM elevation*. *Fifth Domain*. Retrieved 8 March 2018, from https://www.fifthdomain.com/dod/cybercom/2017/10/16/dod-still-working-toward-cybercom-elevation/

Richardson, G. (2012). *The United States Army's Current Capability to Conduct Combined Arms Maneuver* (pp. 37-49). Fort Leavonworth, Kansas: United States Army Command and General Staff College.

Stavridis, J., & Weinstein, D. (2014). Time for a U.S. Cyber Force. *Proceedings Magazine*, (140). Retrieved from https://www.usni.org/magazines/proceedings/2014-01/time-us-cyber-force

Sullivan, J., & Kamensky, D. (2017). How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid. *The Electricity Journal*, *30*(3), 30-35. http://dx.doi.org/10.1016/j.tej.2017.02.006

Timeline of Army Cyber. (2017). *goarmy.com*. Retrieved 8 March 2018, from https://www.goarmy.com/army-cyber/timeline-of-army-cyber.html

U.S. Army Cyber Command. (2016). *Integration of cyberspace capabilities into tactical units*. *www.army.mil*. Retrieved 8 March 2018, from https://www.army.mil/article/163156/integration_of_cyberspace_capabilities_into_tactical_units

U.S. Army Cyber Command | The U.S. Army. (2018). *www.army.mil*. Retrieved 26 March 2018, from https://www.army.mil/armycyber#org-about

Zetter, K. (2014). *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*. *WIRED*. Retrieved 8 March 2018, from https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/