
The Cyber Pandemic has Created Redundancy in the Global Power Competition: Preparing the Defense Industrial Base

Abstract

The global power competition has become increasingly complex and multi-dimensional, driven by the rapid advancement of technology and the emergence of new powers. This competition is now being waged in the cyber domain, where the stakes are high and the consequences are far-reaching. The defense industrial base (DIB) is the backbone of a nation's military capabilities, and it is essential to ensure its resilience and readiness in the face of a cyber pandemic. This paper examines the challenges facing the DIB in the current global power competition and proposes strategies to prepare for a cyber pandemic. The analysis is based on a review of the literature and a series of interviews with experts in the field. The findings indicate that the DIB is currently vulnerable to a cyber pandemic due to its reliance on a small number of suppliers and its lack of redundancy. To address this vulnerability, the DIB must be restructured to include a larger number of suppliers and to ensure that critical capabilities are not concentrated in a single location. Additionally, the DIB must be prepared to respond to a cyber pandemic by having a robust plan in place and by conducting regular drills. The paper concludes that the DIB must be prepared for a cyber pandemic to ensure the security and stability of the global power competition.

Keywords

Introduction

The global power competition has become increasingly complex and multi-dimensional, driven by the rapid advancement of technology and the emergence of new powers. This competition is now being waged in the cyber domain, where the stakes are high and the consequences are far-reaching. The defense industrial base (DIB) is the backbone of a nation's military capabilities, and it is essential to ensure its resilience and readiness in the face of a cyber pandemic. This paper examines the challenges facing the DIB in the current global power competition and proposes strategies to prepare for a cyber pandemic. The analysis is based on a review of the literature and a series of interviews with experts in the field. The findings indicate that the DIB is currently vulnerable to a cyber pandemic due to its reliance on a small number of suppliers and its lack of redundancy. To address this vulnerability, the DIB must be restructured to include a larger number of suppliers and to ensure that critical capabilities are not concentrated in a single location. Additionally, the DIB must be prepared to respond to a cyber pandemic by having a robust plan in place and by conducting regular drills. The paper concludes that the DIB must be prepared for a cyber pandemic to ensure the security and stability of the global power competition.

A. (B)

U. S. Department of Defense, 2020, U. S. A.

C. (A) R.

()

fi ()

M

U

U (1)

(2) () A () ()

U

U

200 | 1

U R , % fi , A

R

fi % %

A R

U % C A M C

% % R | 1/

% % R R

C be rec i Ma i Model Ce i ca ion (CMMC)

% R , % % R , fi

fi % MM

% % fi

C % R

fi fi U U

201 5 % 21. 5 M

4 4 5 01 44 . 5 00/ 111/

U .

A, fi, MM 2.0, MM, U

fi 2.5

10,000

MM 12,000

fi (2.0),

U

fi

Understanding the Traditional DIB and Whistleblowers in a Cyber-Pandemic

2
%

A 1 12,000
% 1/5 1,000
14. % fi

(M) % %

% A % % %

fi (2022,) U

(U MM % U M %

%, ((- % 5 - 2 0(0. 2 5 10000 10 4) 200, 0000 0 51((01 5 5) - 270.00) €1

% fi MM

M \$ 00,000
 MM fi
 (1)
 (2) % %
 (%) %

The Agile Methodology, Patching and Addressing Vulnerabilities

MM fi %
 MM % %
 H %
 MM M
 fi fi fi
 % / 201, % M
 fi % W %
 (%) 1 fi % W
 % 201 21 %
 % U fi
 fi % %
 % W
 MM M2.14, M
 5.0 4, MA 2.111,
 U
 0,000, A %
 % % % W
 U, W
 U H
 A % U
 % 45 U

Conceptual Change of the CMMC Framework

Copyright © 2011 Sage Publications. All rights reserved. DOI: 10.1177/1053426911419811

DIB C Behavior Checklist - Hygiene Score

() /
 MM
 U - fi,
 20. A fi
 MM
 %

Journal of Applied Gerontology 41(3) fi G. W.

M $\frac{R}{M}$ $\frac{fi}{M}$
 $\frac{A}{\%}$ $\frac{M}{\%}$
 $\frac{R}{\%}$ $\frac{MM}{\%}$

U.S. Cybersecurity Strategy for the 2020s. *Journal of Cyber Policy*, 1(1), 1-11. [https://doi.org/10.1016/j.cyp.2020.01.001](#)

11. U.S. Cybersecurity Strategy for the 2020s. *Journal of Cyber Policy*, 1(1), 1-11. [https://doi.org/10.1016/j.cyp.2020.01.001](#)

12. U.S. Cybersecurity Strategy for the 2020s. *Journal of Cyber Policy*, 1(1), 1-11. [https://doi.org/10.1016/j.cyp.2020.01.001](#)

13. U.S. Cybersecurity Strategy for the 2020s. *Journal of Cyber Policy*, 1(1), 1-11. [https://doi.org/10.1016/j.cyp.2020.01.001](#)

14. U.S. Cybersecurity Strategy for the 2020s. *Journal of Cyber Policy*, 1(1), 1-11. [https://doi.org/10.1016/j.cyp.2020.01.001](#)

15. U.S. Cybersecurity Strategy for the 2020s. *Journal of Cyber Policy*, 1(1), 1-11. [https://doi.org/10.1016/j.cyp.2020.01.001](#)

16. U.S. Cybersecurity Strategy for the 2020s. *Journal of Cyber Policy*, 1(1), 1-11. [https://doi.org/10.1016/j.cyp.2020.01.001](#)

17. U.S. Cybersecurity Strategy for the 2020s. *Journal of Cyber Policy*, 1(1), 1-11. [https://doi.org/10.1016/j.cyp.2020.01.001](#)

18. U.S. Cybersecurity Strategy for the 2020s. *Journal of Cyber Policy*, 1(1), 1-11. [https://doi.org/10.1016/j.cyp.2020.01.001](#)

19. U.S. Cybersecurity Strategy for the 2020s. *Journal of Cyber Policy*, 1(1), 1-11. [https://doi.org/10.1016/j.cyp.2020.01.001](#)

20. U.S. Cybersecurity Strategy for the 2020s. *Journal of Cyber Policy*, 1(1), 1-11. [https://doi.org/10.1016/j.cyp.2020.01.001](#)

Special thanks to Joseph C Dorsey for his support and invaluable contributions to this article.

References

1. U.S. Cybersecurity Strategy for the 2020s. *Journal of Cyber Policy*, 1(1), 1-11. [https://doi.org/10.1016/j.cyp.2020.01.001](#)
2. U.S. Cybersecurity Strategy for the 2020s. *Journal of Cyber Policy*, 1(1), 1-11. [https://doi.org/10.1016/j.cyp.2020.01.001](#)
3. U.S. Cybersecurity Strategy for the 2020s. *Journal of Cyber Policy*, 1(1), 1-11. [https://doi.org/10.1016/j.cyp.2020.01.001](#)
4. U.S. Cybersecurity Strategy for the 2020s. *Journal of Cyber Policy*, 1(1), 1-11. [https://doi.org/10.1016/j.cyp.2020.01.001](#)

5.

22. Farhadi, A., Galloway, I., & Beldash, A. (2021). The Impact of Geopolitics on the Middle East. *IEEE Engineering Management Review*, 49(11), 11-15. [DOI: 10.1109/EMR.2021.1011101](#)

23. Farhadi, A. (2020). A New Paradigm for the Middle East. *Connections: The Quarterly Journal*, 19(4), 5-24. [DOI: 10.1109/CONJ.2020.3004515](#)

24. Farhadi, A., Galloway, I., & Beldash, A. (2021). The Impact of Geopolitics on the Middle East. *IEEE Engineering Management Review*, 49(11), 11-15. [DOI: 10.1109/EMR.2021.1011101](#)

25. Farhadi, A. (2020). A New Paradigm for the Middle East. *Connections: The Quarterly Journal*, 19(4), 5-24. [DOI: 10.1109/CONJ.2020.3004515](#)

26. Farhadi, A. (2021). A New Paradigm for the Middle East. *Connections: The Quarterly Journal*, 20(1), 5-24. [DOI: 10.1109/CONJ.2021.3004515](#)

Dr. Adib Farhadi is Assistant Professor and Faculty Director of the Executive Education Program at the University of South Florida. His research focuses on the intersection of geoeconomics, geopolitics, and religion, particularly on the “Silk Road” Central and South Asia (CASA) Region. Dr. Farhadi also serves as the Editor-in-Chief of The Great Power Competition book series and previously served in senior positions for Afghanistan and extensively advised the U.S. government and various other international organizations.

Ian Galloway is a Principle and Management Executive in the Aerospace, Defense, and Energy sector with a keen interest in—and significant experience with—public affairs, international business, strategic consulting, and risk management.

At DGC International (DGCI), he specializes in developing highly innovative solutions that meet client needs in demanding, adverse, and contingency environments. Ian focuses on expanding current services; capturing new business in existing core mission areas; risk management; strategic communication; and corporate development. Recently, he helped to document and refine key supply chain, logistics and program management processes and systems in support of government, military and international commercial markets. As a key member of DGCI’s closely knit and highly collaborative Executive management Team, Mr. Galloway has contributed significantly to the achievements of DGCI.

He travels frequently to maintain his ties to international culture and politics—and his skills to promote the efforts of the Memorial Day Flowers Foundation and Zamani Foundation at home and abroad.

Ayman Beldash serves as a board member of DGCI Corporation, a Virginia-based business that supports the U.S. Government.