Energy Security and Resilience:

Addressing Climate Change and Cyber Threats within DoD Doctrine and Policies

Alexios Antypas and Ion A. Iftimie

The World Economic Forum Global Risks Report singled out climate change and cyber-attacks as the two highest impact and highest likelihood global threats for 2019 (World Economic Forum 2019, 5). This paper looks at the Department of Defense's (DoD) over-dependence on fossil fuels and growing susceptibility to cyber threats within the context of energy security and resilience. The National Defense Authorization Act for Fiscal Year 2018 directed the Secretary of Defense to "ensure the readiness of the armed forces for their military missions by pursuing energy security and energy resilience" (*National Defense Authorization Act for Fiscal Year 2018*). The bill also redefined the terms energy security for DoD as "having assured access to reliable supplies of energy and the ability to protect and deliver sufficient energy to meet mission essential requirements" and energy resilience as "the ability to avoid, prepare for, minimize, adapt to, and recover from anticipated and unanticipated energy disruptions in order to ensure energy availability and reliability sufficient to provide for mission assurance and readiness, including task critical assets and other mission essential operations related to readiness, and to execute or rapidly reestablish mission essential requirements" (Section 2831). We argue that the DoD's energy security and resilience are currently limited by operational dependence on fossil fuels and cyber vulnerabilities of fuel transport infrastructure. The DoD is the largest single energy consumer in America (Warner and Singer 2009), with a consumption of 85 million barrels of liquid petroleum-based fuel at a cost of $8.2 billion in the fiscal year 2017 (Department of Defense 2019). This represents more than 80% of the federal government's total energy consumption (Office of the Assistant Secretary of Defense for Energy, Installations and Environment 2017, 15; Hicks 2017, 3). While the US military "has developed a doctrine, policy and institutional frameworks, and organizational cultural changes in order to begin to break its dependence on oil through energy efficiency" (Antypas 2016, 92), DoD has been unable to decrease its fuel consumption for the past 6 years. Given DoD's global operational requirements, much of its fuel consumption is purchased "as close as possible to the point of use" and the Department of Defense asserted that "as long as the U.S. exercises global leadership in support of our interests, the large volumes of energy needed to enable supporting military capabilities will continue to be purchased overseas and impose risks to the Department" (Office of the Assistant Secretary of Defense for Energy, Installations and Environment 2016, 5). Furthermore, very little has been done by DoD to secure these supply chains from cyber-attacks, despite the fact that DoD acknowledges energy as a

"fundamental enabler of military capability, and the ability of the United States to project and sustain the power necessary for defense depends on the assured delivery of this energy" (Office of the Assistant Secretary of Defense for Energy, Installations and Environment 2016, 3). The second mission of DoD Cyberspace Operations, as defined by Maj Gen Chris "Wedge" Weggeman, Commander of the 24th Air Force/ AFCYBER is to "secure, operate and defend DoD networks and mission systems" (Weggeman 2017), which includes attacks against critical military fuels supply infrastructure. Despite this, of the roughly 133 National Mission, Combat Mission, and Cyber Protection teams and over 6,000 people that make up the DoD's Cyber Mission Force (Weggeman 2017), none are focusing on protecting DoD's fuel supply chains. On May 30, 2018, DoD released the "Managing Cyber Risks to Facility Related Control Systems" memorandum for "Installation Energy Plans (IEPs)". This document addresses the cyber readiness of military installations energy infrastructure (Office of the Assistant Secretary of Defense for Energy, Installations and Environment 2018, G1), but does not address the cyber resilience of operational energy supply chains. This paper concludes that DoD must revisit its 2016 Operational Energy Strategy—which updated the 2011 Operational Energy Strategy—to better address cyber security and dependence on fossil fuels. We also provide a list of recommendations to increase the energy resiliency of the Department while also contributing to an increase in operational capabilities.

Key Words: Operational Energy, Cyber Security, Green Fleet, Department of Defense, Critical Energy Infrastructure Protection

References:

Antypas, Alexios. 2016. "Going Green: The United States Department of Defense and Energy Security." In *Delivering Energy Law and Policy in the EU and the US*, edited by Raphael J. Heffron and Gavin F. M. Little, 92–96. Edinburgh, UK: Edinburgh University Press.

Department of Defense. 2019. "Operational Energy." DoD Office of the Assistant Secretary of Defense for Sustainment. 2019. https://www.acq.osd.mil/eie/OE/OE_index.html.

Hicks, Sierra. 2017. "Powering the Department of Defense Initiatives to Increase Resiliency and Energy Security." American Security Project. https://www.americansecurityproject.org/wp-content/uploads/2017/09/Ref-0204-Powering-the-DoD.pdf.

National Defense Authorization Act for Fiscal Year 2018. 2017. https://www.congress.gov/115/plaws/publ91/PLAW-115publ91.pdf.

Office of the Assistant Secretary of Defense for Energy, Installations and Environment. 2016. "2016 Operational Energy Strategy." Department of Defense.

———. 2017. "Annual Energy Management and Resilience (AEMR) Report Fiscal Year 2016." Department of Defense.

———. 2018. "Department of Defense Annual Energy Management and Resilience Report

(AEMRR) Fiscal Year 2017." 4-DFD4FDC. Department of Defense.

Warner, Jerry, and Peter Warren Singer. 2009. *Fueling the "Balance": A Defense Energy Strategy Primer*. Brookings Institution.

Weggeman, Chris. 2017. "Delivering Outcomes through Cyberspace." presented at the Executive Program in Cybersecurity: The Intersection of Policy and Technology, Harvard University.

World Economic Forum. 2019. "The Global Risks Report 2019." 14. World Economic Forum. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.