Strategic A2/AD in Cyberspace by Alison Lawlor Russell

Reviewed by
Dr. Jan Kallberg and
Cadet Daniel Muncaster

Through a concise and straightforward narrative, Dr. Alison Lawlor Russell outlines the major issues threatening the United States cyber system through the lens of an A2/AD perspective. Alison Russell is an Assistant Professor of Political Science and International Studies at Merrimack College.

How can the people of the United States defend their land and physical assets? This traditional question applies not just to American citizens, but to people across the world and throughout history. A recurring answer is the principle of Anti-Access/Area Denial or A2/AD.

The A2/AD strategy is defined as refusing "movement to a theater (anti-access), while [area denial] affects movement *within* a theater." Putting these ideas into context, A2 would be the US blocking the Soviet Union's access to Cuba with a naval quarantine; AD would be hampering the enemy's ability to maneuver in the Mekong Delta, such as guerilla tactics against US forces in Vietnam.

These strategies represent some of the traditional levels of conflict in cutting communication lines or sequestering the opponent. The world, however, is changing, and conflict changes with it. Cyberspace now plays a crucial role not just in economic and social situations, but also in military communications.

Dr. Russell, in *Strategic A2/AD in Cyberspace,* discusses these concepts and defines cyberspace as one of the current *centers of gravity* around which global strategy now

Dr. Jan Kallberg is Assistant Professor of American Politics in the Department of Social Sciences and Cyber Policy Fellow at the Army Cyber Institute at West Point. He holds a Ph.D. in Public Affairs and a Master's of Political Science from the University of Texas at Dallas; and a JD/LL.M. from Stockholm University. Prior to joining the West Point faculty, Jan was a researcher and Post-Doc at the Cyber Security Research and Education Institute, Erik Jonsson School of Engineering and Computer Science, at the University of Texas at Dallas under Dr. Bhavani Thuraisingham. Dr. Kallberg's research interest is the intersection between public leadership and cyber capabilities; especially offensive cyber operations as an alternative policy option. His personal website is www.cyberdefense.com.

orbits. The Internet, Dr. Russell states, is a significant vulnerability to American society as the primary communications network used for daily life. Within this vulnerability, however, lies the opportunity to leverage power against opponents. Here, Dr. Russell focuses her research entirely on the growing importance of cyberspace and its implications for the global balance of power.

The book is less convincing when it goes through different layers of the Open Systems Interconnection model (OSI model) and puts each layer into the A2/AD context, which might work as a systematic way to approach the topic, but does not carry the discourse the whole way forward. The Internet is designed to trace new routes in a degraded environment, as its core design was tailored to ensure the survivability of information resources in a nuclear war, so the question is whether an adversary could be in total command of the physical layer—the Internet conduit—to execute A2/AD operations. Dr. Russell's *Strategic A2/AD in Cyberspace* has merits in the discourse on whether previous A2/AD discussions have a bearing on cyber and provides a good understanding of how and why A2/AD might be relevant to cyber. The book projects a strategic outlook—the national security perspective—but repeatedly dips into tactical territory, discussing cyber hygiene and minor events. Of the concerns raised in the book, three stand out as highly relevant today: satellites, undersea cables, and electromagnetic pulses. All three are known concerns, but Dr. Russell puts them in another context that is worthy of reflection.

Dr. Russell proposes policy and strategic guidelines to help ensure the United States is well prepared for any attack on its most crucial communications network, and can deter cyber aggression in the future. The book's weakness is that the policy advice

Cadet Daniel Muncaster is a rising Yearling at West Point, and is majoring in International History with a minor in Grand Strategy. This past summer he went to Air Assault School, Cadet Field Training, and the FBI Crisis Negotiation Course held at West Point. He is originally from Joliet, Illinois, and is a member of his Company Sandhurst team. He takes a special interest in cyber warfare and its effect on policy and national security, which he explores with his professor and mentor, Dr. Kallberg. Upon graduation, he hopes to branch Infantry or Military Intelligence.

is generic, and does not add any new viewpoints to the discourse; an example is that there should be investments in the robustness and resilience of the critical infrastructure.

Alison Russell's *Strategic A2/AD in Cyberspace* is worth reading as a short commentary on A2/AD reasoning and serves that purpose well, but its contribution to the cyber discourse is limited.

Strategic A2/AD in Cyberspace

Author: Alison Lawlor Russell

Publisher: Cambridge University Press (February 1, 2017)

Hardcover: 108 pages

Language: English

ISBN-10: 1316629627
ISBN-13: 978-1316629628

Price: $29.00