Small Wars & Insurgencies

ISSN: 0959-2318 (Print) 1743-9558 (Online) Journal homepage: http://www.tandfonline.com/loi/fswi20

Cyber War versus Cyber Realities: Cyber Conflict in the International System

John E. Gudgel

To cite this article: John E. Gudgel (2016) Cyber War versus Cyber Realities: Cyber Conflict in the International System, Small Wars & Insurgencies, 27:3, 550-552, DOI: 10.1080/09592318.2016.1151659

To link to this article: http://dx.doi.org/10.1080/09592318.2016.1151659

Published online: 25 Apr 2016.

SMALL WARS & INSURGENCIES, 2016
VOL. 27, NO. 3, 550–552

Routledge
Taylor & Francis Group

BOOK REVIEW

Cyber War versus Cyber Realities: Cyber Conflict in the International System, by Brandon Valeriano and Ryan C. Maness, New York, Oxford University Press, 2015, ix + 266 pp. ISBN 978-0-19-020479-2

In February 2015, US Director of National Intelligence James Clapper in his annual report to Congress named the cyber threat as the number one strategic threat to the United States, placing it ahead of terrorism, nuclear proliferation, and ISIS.[1] But is the cyber threat really this serious and should the United States reorient its security strategies in response? According to Brandon Valeriano and Ryan Maness in their book *Cyber War versus Cyber Realities*: 'the hype associated with cyber conflict does not meet reality' (p. 226). Defying conventional wisdom expressed by pundits and members of the economically driven 'cyber-industrial complex', they contend that the threat is dangerously overstated, and pushing policy and arms acquisitions in the wrong direction. The stated goal of the book is 'to return the debate on cyber conflict to some measure of rationality and thoughtful theoretical analysis' (p. 17). To counter the hype and bluster, they use theory and empirical evidence to delineate the patterns of cyber conflict since the turn of the century.

Valeriano and Maness view cyber conflict through the lens of international relations and primarily focus on cyber interactions among states and directed towards states in the realm of foreign policy. They argue: 'while cyberspace is a separate domain, it is not unconnected from the normal political domain that is the genesis of conflicts' (p. 15). Following an introductory chapter outlining the contours of the cyber conflict world, eight subsequent chapters build and defend their theoretical framework for the analysis and prediction of cyber conflict in the international system. One of their major conclusions is that 'cyber conflict has not changed how states operate, it has not led to a revolution in military affairs, and the fears associated with the tactic are overblown' (p. 209).

A key component of the authors' framework described in Chapter 3 is their *Theory of Cyber Restraint* that holds that due to fears of collateral damage, blowback, and replication states will restrain themselves from unleashing the full weight of their cyber capabilities. In delineating this theory, Valeriano and Maness stake out a clear middle path between authors such as Richard Clarke and Robert Knake who believe that cyber war has already begun,[2] and Thomas Rid who contends that cyber war will never take place.[3] They frame their approach as *cyber moderation*: the concept that cyber conflict will occur, but that the conflicts themselves will be trivial and will not significantly change state behavior (p. 39). From their theory and approach, they then propose nine hypotheses on interstate cyber interactions.

One of the primary contributions of the authors' research is the construction of an open source and peer-vetted database of cyber incidents and disputes between countries called the Dyadic Cyber Incident and Dispute Dataset (DCID). The 1.0 version of the dataset currently contains 111 cyber incidents (defined as short-term isolated cyber operations) and 45 cyber disputes (defined as longer-term operations that can contain several incidents) between state-to-state rivals over an 11-year period (2001 to 2011) including 21 cyber incidents and 5 cyber disputes between China and the United States. In creating this dataset, the authors recognized the attribution problem and only included incidents and disputes where state-based involvement was explicit and evident (p. 84).

Using this dataset, Valeriano and Maness in Chapters 4 and 5 quantitatively analyze interstate cyber actions including the 'scope, length, and damage inflicted by cyber disputes among rival states' (p. 78) from 2001 to 2011. Some of the research questions they address include: What factors might predict the occurrence, targets, and level of severity in cyber conflict between states? What are the foreign policy implications of cyber conflict? Do cyber incidents influence and lead to more conflictual relations?

What they found was 'that the actual magnitude and pace of cyber disputes among rivals do not match popular perception; only 20 of 126 active rivals have engaged in cyber conflict, and their interactions have been limited in terms of magnitude and frequency' (p. 18). Further, they found that most cyber incidents are regional (e.g. India–Pakistan), focused predominately on espionage and low-level DDoS attacks, and were largely ineffective in getting states to change behavior. There was also little evidence of state-supported or sponsored groups utilizing cyber terrorism. They back up their quantitative data with a series of case studies looking at the most significant recent cyber conflicts involving state (Chapter 6) and non-state (Chapter 7) actors. They then propose a system of rules and norms in cyberspace based on the Just War tradition (Chapter 8).

One criticism of this book is that it appears to marginalize the role of the private sector in national cyber defense. Admittedly, they do state that their primary focus is on government-to-government cyber conflict, and they do devote a chapter to non-state actor cyber incidents. However, many cyber policy scholars including Peter Singer, Martin Libicki, and Jason Healey have emphasized that governments depend on private industry for almost every component of their IT infrastructure,[4] defense of private systems are largely in private hands,[5] and it is the private sector, not governments, that plays the primary role in cyber conflicts.[6]

Overall, this book provides a new perspective on cyber conflict, countering the media hype of impending Cyber Pearl Harbors or Cyber 9/11s. Further, it offers one of the first viable attempts to quantify the impact of cyber actions, and presents facts and evidence to support their theories. As such, they build a strong case for cyber policy based on moderation versus worst-case scenarios.

Notes

1. Taylor, 'James Clapper'.
2. Clarke and Knake, *Cyber War*.
3. Rid, *Cyber War Will Not Take Place*.

4. Singer and Friedman, *Cybersecurity and Cyberwar*, 196.
5. Libicki, *Cyberdeterrence and Cyberwar'*, Kindle Location 1030.
6. Healey, *A Fierce Domain*, Kindle Location 274.

References

Clarke, R., and R. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York, NY: Harper Collins, 2010.

Healey, J., ed. *A Fierce Domain: Conflict in Cyberspace 1986 to 2012*. Kindle Edition. Cyber Conflict Studies Association, 2013.

Libicki, M. *Cyberdeterrence and Cyberwar*. Kindle ed. Santa Monica, CA: RAND Corporation, 2009.

Rid, T. *Cyber War Will Not Take Place*. Kindle ed. New York, NY: Oxford University Press, 2013.

Singer, Peter W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York, NY: Oxford University Press, 2013.

Taylor, G. 'James Clapper, Intel Chief: Cyber Ranks Highest on Worldwide Threats to U.S.' *The Washington Times*, 26 February 2015. http://www.washingtontimes.com/news/2015/feb/26/james-clapper-intel-chief-cyber-ranks-highest-worl/?page=all.

John E. Gudgel
George Mason University, School of Policy, Government & International Affairs, Center for Security Policy Studies (CSPS)
jgudgel@gmu.edu

http://dx.doi.org/10.1080/09592318.2016.1151659