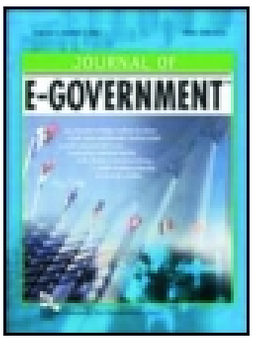

Routledge
Taylor & Francis Group

Journal of Information Technology & Politics

ISSN: 1933-1681 (Print) 1933-169X (Online) Journal homepage: http://www.tandfonline.com/loi/witp20

Cyber War Versus Cyber Realities: Cyber Conflict in the International System. By Brandon Valeriano and Ryan C. Maness

Francis C. Domingo

To cite this article: Francis C. Domingo (2015): Cyber War Versus Cyber Realities: Cyber Conflict in the International System. By Brandon Valeriano and Ryan C. Maness, Journal of Information Technology & Politics, DOI: 10.1080/19331681.2015.1101039

To link to this article: http://dx.doi.org/10.1080/19331681.2015.1101039

Accepted author version posted online: 18 Nov 2015.

CYBER WAR VERSUS CYBER REALITIES: CYBER CONFLICT IN THE INTERNATIONAL SYSTEM.

Francis C. Domingo

De La Salle University and the University of Nottingham

CYBER WAR VERSUS CYBER REALITIES: CYBER CONFLICT IN THE INTERNATIONAL SYSTEM. By Brandon Valeriano and Ryan C. Maness. New York, NY: Oxford University Press, 2015, 288 pages. ISBN: 9780190204792

Cyberspace has evolved into a domain of international conflict as well as a source of threat inflation by the policy makers and the media. The hype over conflict in cyberspace is reflected predominantly in the literature in International Relations where a substantial amount of work emphasizes the consequences of conflict without the benefit of empirical evidence. This misleading discourse is problematic because it can generate confusion and suspicion between governments, consequently influencing interactions between states in the international system. Given the prevailing literature, there is a need for more nuanced studies that are grounded on social science and empirical realities.

This scholarship gap is addressed in Brandon Valeriano and Ryan Maness' much needed book *Cyber War Versus Cyber Realities* where they contend that cyber incidents have not escalated to

the hyperbolic propositions that many companies and pundits would have people believe. The book makes a persuasive argument that challenges existing knowledge: cyber interactions between states can be characterized by restraint and regionalism. Valeriano and Maness develop a theory of cyber conflict based on the concept of deterrence or the prevention of the use of extreme measures due to the fear of retaliation and escalation beyond control (p. 56). Since the authors are convinced that deterrence is an illogical concept when applied to cyber operations, they maintain that concept of restraint is more appropriate in interpreting the dynamics of state interactions (p. 60).

The authors substantiate their theory by presenting extensive data on cyber incidents and disputes between states engaged in rivalries (chapter 4). To understand how states have used cyber tactics, the chapter examines all information on cyber interactions between rival states during the last decade and identifies patterns of cyber conflict. Based on the data, the magnitude and pace of cyber disputes among rival states are not consistent with popular perception. In fact, only 20 out of 126 active state rivals have engaged in cyber conflict and interactions have been limited in terms of magnitude and frequency (pp. 89-90).

The book then investigates the foreign policy implications of cyber conflict when the tactic is used as an instrument (chapter 5). In analyzing the dataset, the authors demonstrate that most cyber incidents and disputes have no impact on general interstate relations. They discover that only one type of incident (distributed denial of service) inflicted negative consequences on the conflict-cooperation interaction of states (p. 127). The chapter also shows that cyber incidents

and disputes between regional rivals lead to negative foreign policy responses and have significant impacts on foreign policy when the United States is involved (pp. 128-129).

The authors observe with similar findings when they scrutinize the most prominent cyber incidents between states in chapter 6 and assess the most sophisticated incidents executed by non-state actors in chapter 7. An evaluation of three cases – *Bronze Solider*, *Stuxnet*, and *Shamoon* - revealed that these incidents had no significant impact on state interaction and that the incidents were greatly exaggerated as threats by the media and pundits (p. 161). On the other hand, while non-state groups were successful in imposing fear and insecurity among governments, the actual impact of the incidents on state behavior was minimal to non-existent (pp. 185-186). A more significant consequence of non-state actions is the overreaction of states to these threats, therefore leading to the employment of cyber security firms.

The last substantial chapter draws on the Just War tradition to examine the system of rules and norms in cyberspace (chapter 8). The authors argue that existing guidelines for cyberspace such as the Tallinn Manual are not applicable because they are based on the assumptions (i.e. mutuality and consent in war), which do not necessarily apply to cyber conflict (p. 198). When rules and norms are applied in cyberspace, the goal according to the authors should be to institutionalize the perspective that cyber weapons are a prohibited taboo, preventing the further damage already initiated by state so far (pp. 196-197). Developing a system of guidance for cyber operations based on moral and ethical actions is therefore a step towards the right direction.

Cyber War Versus Cyber Realities is a groundbreaking empirical work and a necessary read for scholars focusing on cyber conflict and people generally interested in international relations.

The book makes at least four significant contributions to the literature in International Relations. First, the book provides a thorough discussion regarding the terms and concepts essential to the study of cyber conflict. Considering that cyber security is a new branch of scholarship, an introduction of new concepts and refinement of existing ideas is critical for the advancement of the field. Second, the book makes use of mix methods to develop compelling explanations about cyber interactions between states. This makes the book unique since most of the studies on the topic are qualitative in nature partly due to the lack of access to relevant data as well as the insufficient cases that can be observed (Liff 2012, Kello 2013).

Third, scholars note that existing work on cyber conflict are generally disorganized and do not engage with the wider literature in International Relations Theory (Eriksson and Giacomello 2007, Dunn Cavelty 2013). In this context, the book makes an important contribution since it proposes a theory that builds on social constructivism. The authors contend that the choice to execute a cyber operation is socially constructed by the situation of rivalry, the system of norms in operation, and the fear-based responses in the threatened society. Therefore, the authors' theory is based on the notion that cyber responses are "conditioned by engagement with reality, and this engagement is a function of the time, location, and the system in operation" (p. 51). Fourth, the book discredits the misleading perceptions about the impact of cyber incidents and disputes on the foreign policy behavior of states. This is a crucial because it can possibly influence policy makers and military leaders to reevaluate their responses to cyber incidents and avoid the hype that has influenced the overreaction to cyber conflict.

There book however needs further clarification in two main areas. The first point is about the application of existing theories to explain cyber phenomena. The authors argue: "Applying old theories from different contexts is of limited value in the cyber discourse, as new ideas and concepts need to be brought to the forefront to explain the dynamics of cyber conflict" (p. 54). While this point is valid in the case of state rivalries, previous work by Eriksson and Giacomello (2007), Saltzman (2013), Lawson (2013), Ebert and Maurer (2013) and Russell (2014) suggests that existing International Relations theories have appropriate explanatory power to account for state interactions in cyberspace.

The second point pertains to the selection of state rivals. The authors maintain that "States that act without serial competition act in a different manner from rivals…" but do not clarify the basis for this claim (p. 53). Does this imply that states not involved in conflict rivalries are less likely to engage in cyber conflict? Why then do state continue to develop cyber capabilities? The book is unclear in addressing these points, therefore leaving room for further scholarship in field of cyber security. While there is certainly much work to be done, Valeriano and Maness have provided scholars with an impressive starting point that contributes towards greater understanding of the cyber security threat landscape as well as the prospects of a less threatening cyber future.

Francis C. Domingo

De La Salle University and the

University of Nottingham

REFERENCES

Dunn Cavelty, M. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review* 15(1): 105-122.

Ebert, H. and Maurer, T. (2013) Contested Cyberspace and Rising Powers *Third World Quarterly*, 34 (6): 1054-1074.

Eriksson, J. and Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR) Relevant Theory? *International Political Science Review* 27 (3): 221-244.

Kello, L. (2013). The Meaning of the Cyber Revolution. *International Security* 38(2): 7-40.

Lawson, S. (2013). Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats *Journal of Information Technology & Politics* 10(1): 86–103.

Liff, A. (2012). Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies*, 35 (3): 401-428.

Russell, A. L. (2014). *Cyber Blockades*. Washington D.C.: Georgetown University Press.

Saltzman, Ilai (2013). Cyber Posturing and the Offense-Defense Balance, *Contemporary Security Policy*, 34(1): 40-63.