Journal of Strategic Security

Volume 13 | Number 2 Article 9

International Relations in the Cyber Age: The Co-Evolution Dilemma. By Nazli Choucri and David Clark. Cambridge, MA: MIT Press, 2018.

Mark T. Peters
USAF, Retired

pp. 125-128

Recommended Citation
Peters, Mark T.. "International Relations in the Cyber Age: The Co-Evolution Dilemma. By Nazli Choucri and David Clark. Cambridge, MA: MIT Press, 2018.." *Journal of Strategic Security* 13, no. 2 (2020) : 125-128.
DOI: https://doi.org/10.5038/1944-0472.13.2.1842
Available at: https://scholarcommons.usf.edu/jss/vol13/iss2/9

International Relations in the Cyber Age: The Co-Evolution Dilemma. By Nazli Choucri and David Clark. Cambridge, MA: MIT Press, 2018.

International Relations in the Cyber Age: The Co-Evolution Dilemma. By Nazli Choucri and David Clark. Cambridge, MA: MIT Press, 2018. ISBN: 9780262038911. Charts. Graphs. Appendices. Pp. vii, 420. $45.00.

Those writing about cyberspace often become mired in technical details and fail to address the societal and political changes driven by network policy, internet accessibility, or security standards. Nazli Choucri and David Clark avoid this trap during *International Relations in the Cyber Age* by delivering a comprehensive look at how state and non-state entities interact despite a strong technical foundation. Dr. Choucri follows on her earlier 2012 groundwork published by MIT, *Cyberpolitics in International Relations,* while integrating her co-author to deliver a unique analytical framework as well as model multiple cases. Simply put, the framework compares a modified Open Systems Interconnection (OSI) architecture against a slightly expanded, Kenneth Waltz political structure to allow visualizing cyber influences on local and global outcomes. The book presents two clear sections, the first explaining the model and the second conducting application through several governance case studies. Any simplification offered here fails to demonstrate the same elegant complexity and enhanced understanding provided throughout this text. Wonderfully detailed with an abundance of diagrams, charts, maps and studies, all individuals working in international policy, cyber policy, or even intelligence analysis, should move this book to the top of their reading list.

Many international relations texts begin by comparing the newly presented model to more well-known options. This analysis proves no different when identifying four interacting levels as individual, state, international, and global, the modified Waltz approach while describing how these areas experience lateral societal pressures from national interaction between population, resource and technology influences. Choucri and Clark apply these parameters describing cyber changes through their analytical tool. The matrix and associated overlay compares architecture elements (People, Information, Application, Services, Internet, and Physical) against governance considerations (providers, suppliers, standards, international policy, and governments) with

overarching categories (businesses, citizens, non-governmental organizations, and illegitimates). This structure sounds confusing and complex when described textually but diagrammed analysis proves remarkably comprehendible. Further, as one begins to visualize cases through the matrix, the text's second half expands by adding a control points analysis to the demonstrated flows. The extended product illuminates where societies face pressure as well as possible solutions.

As with all good beginnings, Choucri and Clark initially create the policy student's solid foundation. The process first socializes a cyberspace framework before integrating OSI-architectural elements with state level-lateral pressure models. All states fit into six profiles based on how resource(R), population(P) and technology (T) variables create influence based on a 'greater than' order to those same variables, such as population over technology over resources (PTR). This would show the state faces the most pressure from population concerns and the least pressure from access to resources. Accumulated data from previous World Bank studies comparing states shows China faces the most lateral pressure as a PTR state while the U.S. faces the second most as a TRP state. Throughout the text, anywhere significant math or statistics were incorporated, the authors include a detailed appendix discussing data collection and analysis. Once the analytical model is created, the final chapter for this section evaluates lateral cyber pressure differently than the previous standard by focusing on technical considerations such as undersea cables, IPv6 transitions, and internet service delivery.

The text's middle part transitions to the work's main arguments, demonstrating control points made apparent through applying the presented framework and discussing several cyber policy, co-evolution use cases. Control point analysis maps how various internet systems function through identifying where processes may be influenced by who controls actions at each level. These diagrams are probably the book's strongest point, clearly showing how any internet process can be traced to identified control points, and those points linked to a matrixed, governance framework. Choucri and Clark evaluate a typical U.S. Internet service as well as standard U.S. and Chinese internet provider practices. Backing up slightly, the two include the nearly mandatory historical cyberattack chapter categorized as three cyberspace conflict types: conflict over space management, conflict over strategic advantage, and conflicts over national

https://scholarcommons.usf.edu/jss/vol13/iss2/9
DOI: https://doi.org/10.5038/1944-0472.13.2.1842

security issues. Identifying these issues allows calling out national and international organizations that might or currently are pursuing mitigations. Finally, and most importantly, several future governance platform goals appear: creating a metaview about espionage data, being able to quantify effects across multiple attacks, and improving analytical capes for cyberthreat assessment. While many authors have touched on these points over time, one of the biggest challenges remains settling on a community standard where data can be exchanged and evaluated.

The book's remainder returns the focus to governance processes and international cyberspace development through co-evolution, or, how cyberspace may develop coordinated processes through a theory of change. The *Talinn Manual 2.0* network analysis view aligning over 150 cyberspace laws simply excels, highlighting the efficacy of the textual model. The careful analysis and connections show application through situations, doctrine, and policy with a goal to potentially predict network wide changes. Some key discussion issues include cyberspace access, network stability, and digital society. The authors leave the readers with five key imperatives about co-evolution: Cyber-IR systems provide fundamental context, routinely revisiting state roles, evaluating who controls sustaining processes, identifying changing security threats, and finally, recognizing how cyber as a social system impacts all human interactions. While each imperative could lead to a further volume in and of itself, the text admirably links together these complicated concepts for the time being.

Typically, a book review might suggest flaws in the author's logic, elements for improvement, or complaints about construction, but this read was outstanding from start to finish. *International Relations in the Cyber Age* was excellently written, referenced, and assembled, expertly structured to include both beginning and advanced readers, and possessed multiple charts and graphs to visually explain difficult topics. My largest complaint, was the author's repeatedly referral to the, "Red Queen's Hypothesis" and I found myself looking it up multiple times. The Red Queen's Hypotheses posits that creatures or actors slow to adapt to change may be out-evolved and no longer fit for their environment. One other minor complaint dealt with the authors creating their own internet layer model rather than using the TCP/IP four-layer model or the OSI seven-layer model. Those two models appear frequently during technical

evaluations and could have more tightly tied technical security and network experts to the international relations conclusions presented here.

Overall, *International Relations in the Cyber Age: The Co-Evolution Dilemma* offers an excellent perspective as either an addition to one's own knowledge or as a teaching foundation for almost any college class level. The two authors create a well-reasoned argument, meld together multiple options to present an analytical framework, and then apply the framework to multiple case studies. The text then extrapolates how understanding those cyberspace studies influence future international relations between actors at all levels. Thoroughly researched, with a multitude of additional references presented as appendices, diagrams, and charts, this book should be immediately purchased and read by any cyber-practitioner, whether technically or policy oriented as it is one of the best cyberspace politics analyses have read in quite some time.

Mark T. Peters II, USAF, Retired

https://scholarcommons.usf.edu/jss/vol13/iss2/9
DOI: https://doi.org/10.5038/1944-0472.13.2.1842