[Book Review]
On Cyber: Towards an Operational Art for Cyber Conflict

Review by James Caroland, Editor-in-Chief, Cyber Magazine

On War is one of the preeminent books on military strategy and war and is practically required reading for any officer in the United States military, as well as many international militaries. You will find it in curriculums at Service and National War Colleges where warfare is studied, and any officer who has completed their Joint Professional Military Education (JPME) probably has a copy on their bookshelf. I can see my tattered, dog-eared copy from across my office as I write this. *On War* was written by Prussian General Carl von Clausewitz … in the early 1800s … long before the Advanced Research Projects Agency (ARPA) invented what came to be known as the Internet.

Fast forward over a century and a half to encounter ubiquitous cyberspace, its designation as the fifth domain of warfare, and the creation of military commands for cyber warfare. Cyber conflict has already been happening for over a decade. While there have been many articles written about various aspects of cyber conflict over that time, there has not been a comprehensive book that addresses how militaries defend, fight, and win in cyberspace – until now.

With a title that I assume is a nod to Clausewitz's *On War*, Gregory Conti and David Raymond have written *On Cyber: Towards an Operational Art for Cyber Conflict*, updating Clausewitz's teachings (among others) to account for the advent of cyberspace. With cyber conflict being primarily -- though not exclusively -- a military realm, the foundation of the book is a lot of military doctrine. However, Conti and Raymond are able to take the language of warfighting and make it accessible to a non-military audience. They logically organize the book by the various elements of combat (terrain, maneuver, intelligence, command and control, etc.); address each of these across the strategic, operational, and tactical levels of war; and explain how each relates to and can be leveraged in cyber conflict.

Conti and Raymond creatively balance quoting historical military strategists (e.g., Clausewitz, Jomini, Sun Tzu, Napolean, Patton) and discussions of traditional warfighting (e.g., Battle of Marathon (490 BC), Civil War, World Wars I/II) with quoting modern day cybersecurity professionals (e.g., Dan Kaminsky, the grugq, Whitfield Diffie, Dan Geer) and discussions of recent cyber events. There are sometimes two camps in the cyber versus kinetic warfighting debate – those that say cyber can be applied to any kinetic warfighting concept and those that say cyber is completely unique. Conti and Raymond caution either camp in dismissing the other and do a credible job presenting how traditional kinetic warfighting may or may not apply in cyber conflict, providing concrete examples, illustrative graphs and tables, and well-researched points to make their cases and recommendations.

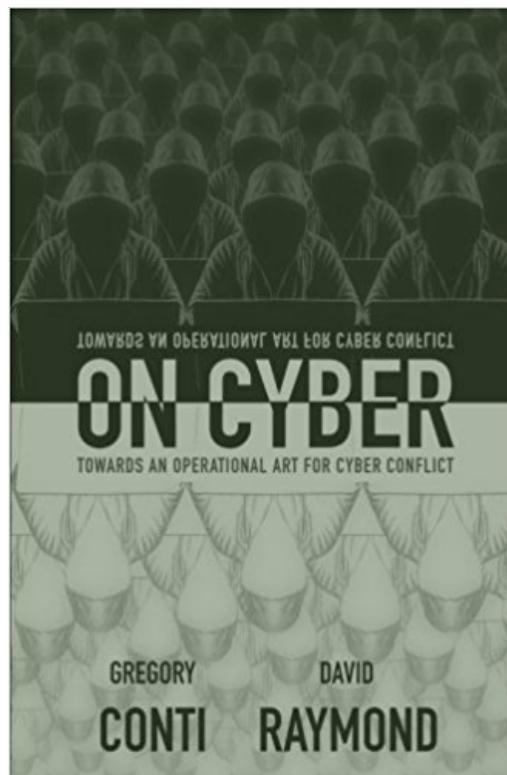The book is certainly not without its references to geek culture, which is appreciated by many of us in the cyber community. These include books, movies, comics, and television shows such as Star Trek, The Matrix, Harry Potter, Ender's Game, Robocop, The Terminator, and X-Men, as well as nerdcore music lyrics. Although, I was a little sad to see Star Wars did not make the cut. These references are not simply randomly inserted, but deliberately used to elucidate some facet of cyber conflict in a clever way.

Other than hoping for a Star Wars allusion, as a Naval officer, I personally was hoping for more Navy context (along with the other military services). Although there is mention of the Phalanx weapons system found on Navy ships, the book is rather Army-centric in its context. This isn't surprising as Conti and Raymond are retired Army officers with over 50 years of service combined. At the same time, you don't have to be in the military to understand the book. It is extremely well-researched with 693 endnotes and has many footnotes throughout its pages explaining various concepts, both military and cyber related.

Conti and Raymond also highlight several key themes that are integrated throughout the book such as automation in cyber conflict is key, speed matters in cyberspace, attribution is hard, laws and policy can be limiting (for the good guys), modern technology influences decisions, geography is "different" in cyber conflict, and command and control is more than just humans. If for some reason you choose not to read the entire book, you can always skip to the end of each chapter which has conclusions and recommendations that effectively tie together concepts from the chapter.

The book ends with "A Look at the Future". While this final chapter does an excellent job covering technology on the horizon and potential ramifications for cyber conflict, it also emphasizes that cyber conflict is more than just technology. It addresses creating an agile culture, having multi-disciplinary teams, adapting cyber institutions, growing cyber talent, and updating doctrine.

I highly recommend this educational, entertaining, and insightful book to anyone interested in cyber conflict/warfare. Military and government members, particularly senior leaders, strategists, planners, and decision-makers, should order their copy now. Much like my copy of *On War*, *On Cyber: Towards an Operational Art for Cyber Conflict* will undoubtedly become tattered and dog-eared from reference and use.