

Foreword

The International Law Studies “Blue Book” series was initiated by the Naval War College in 1901 to publish essays, treatises, and articles that contribute to the broader understanding of international law. This, the seventy-sixth volume of the series, consists of papers written for the Naval War College’s Symposium on Computer Network Attack and International Law.

Participants in the Symposium represented a broad range of expertise in the rapidly developing field of information operations. Included were government officials, operational commanders, international law scholars, technical experts, and military and civilian lawyers. They were brought together to examine the expanding capabilities created for military planners by the technological revolution that today permits means and methods of attack beyond the contemplation of war-fighters of the past. This Symposium focused on one of those—computer network attack. Although its full potential is still unrealized, it will certainly become an integral part of the way warfare is waged. Because of its unique nature, computer network attack presents difficult challenges to the law. Yet, if it is to be useful to the operational commander, these challenges must be addressed and the issues surrounding when and how it may be used resolved. Although much work remains to be done, this Symposium has that process well underway.

While the opinions expressed in this volume are those of the individual writers and not necessarily those of the United States Navy or the Naval War College, their insightful analyses make a valuable contribution to the study and development of the law applicable to computer network attack. On behalf of the Secretary of the Navy, the Chief of Naval Operations, and the Commandant of the Marine Corps, I extend to all the contributing authors our thanks and gratitude, with a special note of appreciation to Professor Michael N. Schmitt and Lieutenant Commander Brian T. O’Donnell, who not only contributed individual papers, but provided invaluable service as the editors of this important publication.

RODNEY P. REMPT
Rear Admiral, U.S. Navy
President, Naval War College

Introduction

The 1990's produced a worldwide, technological explosion in computers, information processing, communication systems, and the use of the Internet. The global reach of these vast and complex networks pervades almost every aspect of modern civilization. The Naval War College conducted a Symposium on Computer Network Attack and International Law in June 1999, to address such advanced technology's impact in the area of warfare directed through and against computer networks. The Symposium is documented in this volume of the International Law Studies (the "Blue Book") series.

The Symposium was made possible with the support of the Honorable Arthur L. Money, Assistant Secretary of Defense (Command, Control, Communication, and Intelligence) and the Pell Center for International Relations and Public Policy of Salve Regina University, Newport, Rhode Island. Their assistance is greatly appreciated.

Professor Michael N. Schmitt, George C. Marshall European Center for Security Studies and Lieutenant Commander Brian T. O'Donnell, JAGC, US Navy, Navy Warfare Development Command, collaborated as editors for this volume. Mike was a member of the Oceans Law and Policy Department, (now the International Law Department) before retiring from the US Air Force. Brian was also a member of our Department prior to his transfer to the Navy Warfare Development Command. Their dedication and perseverance are responsible for seeing this project to completion.

A special thank you is necessary to Dr. Robert S. Wood, the former Dean of the Center for Naval Warfare Studies, and Dr. Alberto Coll, the current Dean, for their leadership and support in the planning and conduct of the Symposium, and the funding for the printing of this book.

The "Blue Book" series is published by the Naval War College and distributed throughout the world to academic institutions, libraries, and both US and foreign military commands. This volume is a fitting and necessary addition to the series as it begins its second century of publication.

DENNIS MANDSAGER
Professor of Law
Chairman, International
Law Department

Preface

This volume of the International Law Studies series (“Blue Books”) completes work begun in June of 1999 during the United States Naval War College’s Symposium on Computer Network Attack and International Law. Gathering international legal scholars, judge advocates, warfighters, and computer experts under the auspices of the Oceans Law and Policy (now International Law) Department, the symposium comprehensively considered an emerging *means*, the computer, and *method*, computer network attack, of warfare.

At the time, numerous countries, most notably the United States, were beginning to develop computer network attack (CNA) capabilities. Simultaneously, there was a growing global sense of vulnerability to computer network attack, not only from State actors, but also terrorists, criminals, and cybervandals. Unfortunately, thinking on the technical possibilities of CNA was far outpacing that on the legal limitations to which such methods and means were (or should be) subject. Narrowing this gap was the symposium’s purpose, and that of this volume. By bringing operators, technicians, and lawyers together, a fertile environment was created in which those responsible for designing and conducting CNA could acquire a more sophisticated understanding of the normative limits on their activities, while those tasked with considering prescriptive constraints became better equipped to grasp the context in which the law is to be applied. Simply put, the intent of both the symposium and this book was to relate the possible to the permissible.

In 1999 the nature of international law’s applicability to computer network attack was quite uncertain. Despite the increasing attention paid to the issue since then, much uncertainty remains. This volume addresses the most pressing issues. It begins with contributions describing the operational milieu in which the law applies, including its technical possibilities and strategic significance. The focus then shifts to the law. Most significant is the legal analysis of the *jus ad bellum*, that aspect of international law governing when a State may resort to force as an instrument of national policy. Does a computer network attack violate the prohibition on the use of force found in Article 2(4) of the United Nations Charter, and, if so, when? Can it fall within one of the two exceptions to that proscription—use pursuant to Security Council authorization in accordance with Chapter VII of the Charter and use in self-defense, based either on Charter

Article 51 or the customary right thereto? If a State conducts a CNA against another State, can the target respond with classic kinetic force? If so, under what circumstances?

Equally challenging are the *jus in bello* issues, i.e., those that surround the conduct of hostilities. When does the law of armed conflict (LOAC) apply to CNA operations? Is it implicated in all cases of computer network attack or do some fall outside its purview? Does it present difficulties for the application of core LOAC principles like discrimination and proportionality or pose particular risks to protected persons and objects? Do lacunae exist in a normative architecture intended to shield non-participants from the effects of conflict? Might CNA, by contrast, offer possibilities for enhancing their protection?

Complex questions regarding computer network attack extend beyond the confines of the *jus ad bellum* and *jus in bello*. This “Blue Book” explores the key ones. Specific attention is devoted, for instance, to the topics of neutrality, space operations, intelligence gathering, and terrorism. Additionally, both the suitability of existing treaty law and application of rules of engagement are considered.

Given the uncertainty surrounding the precise legal limitations on computer network attack, considerable interpretive play exists. Paradoxically, those States most capable of integrating computer network attack, or more broadly information warfare, into their operational capabilities, are those with the greatest vulnerability to CNA. Thus, they find themselves on the horns of a dilemma—resist constraints on the technology and thereby heighten opportunity *and* threat, or normatively impede it and forfeit asymmetrical advantage out of concern over asymmetrical risk. Conversely, those States most defenseless against computer network attack might well find developing a CNA capability attractive because doing so is relatively inexpensive compared to acquiring the conventional military capabilities necessary to challenge those who are currently dominant militarily. How States resolve these policy Catch-22s will determine much of the face of future conflict and its legal infrastructure.

Many thanks are due in any major publishing project, a fact especially true in this one. First and foremost are those earned by the contributors to the volume. Aside from the insightful analysis for which readers are in their debt, they were paragons of patience and cooperation during the unfortunate delays that accompanied completion of the project. Secondly, Captain Ralph Thomas (USN, retired) selflessly gave of his own time to editing this work. His name would have appeared on the title page, but for his excessive modesty. Professor Emeritus Jack Grunawalt also contributed substantial time editing and reviewing the chapters for their content. Lieutenant Colonel James Meyen, USMC, assisted in editing and brought his past experience in bringing this volume to print. Particular

gratitude is due to Professor Dennis Mandsager and the entire staff of the College's International Law Department, Ms. Pat Goodrich of the Naval War College Press, who served as the Press' project editor, as well as Mr. Samuel O. Johnson, Mr. Jeremiah Lenihan, Ms. Susan Meyer, and Ms. Joan Vredenburg for desktop publishing and proofreading support.

Hopefully, this collection of articles will assist in elucidating the intricacies of applying international law to computer network attack. Perhaps as important is the desire to have it assist in the process of determining appropriate normative vectors as the relevant law evolves to meet these new capabilities. CNA offers both promise and peril. Understanding it, and the legal environment in which it operates, is essential if computer network attack is to contribute to international stability and humanitarian protection. Regardless of the allure of CNA for those starstruck by its possibilities, ultimately the objective of operators and attorney must be to further such ends.

Michael N. Schmitt

Professor of Law

George C. Marshall European

Center for Security Studies

Garmisch-Partenkirchen, Germany

Brian T. O'Donnell

LCDR, JAGC, USN

Legal Advisor

Navy Warfare Development Command

Newport, Rhode Island