SSI
STRATEGIC STUDIES INSTITUTE

Executive Summary

Strategic Studies Institute and U.S. Army War College Press

UNITED STATES ARMY WAR COLLEGE PRESS
Carlisle Barracks, PA
STRENGTH—WISDOM

LEGALITY IN CYBERSPACE: AN ADVERSARY VIEW

Keir Giles
with
Andrew Monaghan

The United States and its allies are in general agreement on the legal status of conflict in cyberspace. Although key principles remain unresolved, such as what precisely constitutes an armed attack or use of force in cyberspace, overall there is a broad legal consensus among Euro-Atlantic nations, that existing international law and international commitments are sufficient to regulate cyber conflict.

This principle is described in a range of authoritative legal commentaries. But these can imply misleadingly that this consensus is global and unchallenged. In fact, China, Russia, and a number of like-minded nations have an entirely different concept of the applicability of international law to cyberspace as a whole, including to the nature of conflict within it. These nations could therefore potentially operate in cyberspace according to entirely different understandings of what is permissible under international humanitarian law, the law of armed conflict, and other legal baskets governing conduct during hostilities.

U.S. policymakers cannot afford to underestimate the extent to which Russian concepts and approaches differ from what they may take for granted. This includes the specific question of when, or whether, hostile action in cyberspace constitutes an act or state of war. Recent Russian academic and military commentary stresses the blurring of the distinction between war and peace, and asks to what extent this distinction still exists. This suggestion of a shifting boundary between war and peace is directly relevant to consideration of at what point Russia considers itself to be at war and therefore subject to specific legal constraints on actions in cyberspace.

Conversely, a range of actions that are considered innocent and friendly by the United States and European nations are parsed as hostile actions by Russia, leading to Russian attempts to outlaw "interference in another state's information space." The Russian notion of what constitutes a cyber weapon—or in Russian terminology, an information weapon—is radically different from our assumptions.

Initiatives put forward by Russia for international cooperation on legal initiatives governing cyber activity have received a mixed response from other states. But they need to be taken into account because of the alternative consensus on cyber security opposing the views of the United States and its close allies, which is growing as a result of an effective Russian program of ticking up support for Moscow's proposals from third countries around the world.

This monograph explores the Russian approach to legal constraints governing actions in cyberspace within the broader framework of the Russian understanding of the nature of international law and commitments, with the aim of informing U.S. military and civilian policymakers of views held by a potential adversary in cyberspace. Using a Russian perspective to examine the legal status of a range of activities in cyberspace, including what constitutes hostile activity, demonstrates that assumptions commonly held in the United States may need to be adjusted to counter effectively—or engage with—Russian cyber initiatives.

*****

More information about the programs of the Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press may be found on the Institute's homepage at *www.StrategicStudiesInstitute.army.mil.*

*****

Organizations interested in reprinting this or other SSI and USAWC Press executive summaries should contact the Editor for Production via e-mail at *SSI_Publishing@conus.army.mil.* All organizations granted this right must include the following statement: "Reprinted with permission of the Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College."

This Publication

SSI Website

USAWC Website