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 and WISDOM

PROSPECTS FOR THE RULE OF LAW IN CYBERSPACE

Keir Giles

This Letort Paper provides an overview of moves toward establishing international norms and the rule of law in cyberspace, and the potential for establishing further internationally accepted and enforceable standards of behavior. Completed in late 2015, it reflects the state of play in these areas at that time. It especially highlights opposing views on the nature of legality in cyberspace, and how and where those views are gaining global support.

The United States believes, in broad terms, that activities in cyberspace require no new legislation, and that existing legal obligations are sufficient. However, a large number of other states led by Russia and China believe that new international legal instruments are essential in order to govern information security overall, including as expressed through the evolving domain of cyberspace. Russia in particular argues that the challenges presented by cyberspace are too urgent to wait for customary law to develop as it has done in other domains; instead, urgent action is needed.

As well as disagreement on new legislation, there is a fundamental schism in international discussion on what exactly should constitute illegal behavior in cyberspace. Russian and Chinese information security policies express a holistic approach to countering information threats, particularly by recognizing the problem of harmful content, as well as the strict "cyber" issue of harmful code or "cyber weapons." Nevertheless, the previous basic Euro-Atlantic assumption that freedom of expression and free movement of information online are sacrosanct has now been challenged in some quarters, in the face of their exploitation by Russia and the Islamic State (IS). Hostile information activities by both actors have brought clarity to the concerns over subversive content that were previously expressed by Russia and China but disavowed by the United States.

Another keystone element of the ongoing legal debate is whether, when, and to what extent the Law Of Armed Conflict (LOAC) can apply to hostile actions carried out through cyberspace, and hence the sub-topic of what precisely constitutes an "armed attack" online. This Letort Paper provides an overview of the current state of the debate and progress toward international agreement, including a discussion of the *Tallinn Manual on the International Law Applicable to Cyber Warfare,* and its merits and limitations.

Further sections of this Letort Paper discuss existing rules and agreements governing cyber activity, including attempts to control cyber weapons by the Wassenaar Arrangements—an international regime regulating exports of conventional weapons and sensitive dual-use items and technologies with military end-uses—and the development of a range of international confidence building measures (CBMs) in various international organizations, including the Organization for Security and Co-operation in Europe (OSCE), the Organization of American States (OAS), the Shanghai Cooperation Organization (SCO), and more. Besides CBMs, several other codes of norms and good behavior have been constructed in regional agreements and are reviewed here, including the Council of

Europe Convention on Cybercrime (the Budapest Convention). A further section discusses bilateral agreements and treaties, including those between the United States and Russia, and the United States and China.

This Letort Paper concludes with policy recommendations, including the key conclusion that adversaries are framing their cyber offensive potential in an entirely different mental construct than that which applies in the United States and its Western allies. The approaches of key potential state adversaries to legitimation or prohibition of online activity provides important clues to how they see this activity in terms of their own behaviors. As such, they provide a useful aid in planning for, countering, and responding to the wide range of threats to U.S. security that state and nonstate adversaries can present using the Internet.

*****

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