CYBERTERRORISM AND COMPUTER CRIMES: ISSUES SURROUNDING THE ESTABLISHMENT OF AN INTERNATIONAL LEGAL REGIME

Richard W. Aldrich

INSS Occasional Paper 32

Information Operations Series

April 2000

USAF Institute for National Security Studies
USAF Academy, Colorado

The views expressed in this paper are those of the authors and do not necessarily reflect the official policy or position of the Department of the Air Force, the Department of Defense, or the U.S. Government. This paper is approved for public release by SAF/PAS; distribution is unlimited.

****

Comments pertaining to this paper are invited; please forward to:
Director, USAF Institute for National Security Studies
HQ USAFA/DFES
2354 Fairchild Drive, Suite 5L27
USAF Academy, CO 80840
phone: 719-333-2717
fax: 719-333-2716
email: james.smith@usafa.af.mil

Visit the Institute for National Security Studies home page at
http://www.usafa.af.mil/inss

TABLE OF CONTENTS

Foreword vii

Executive Summary ix

Introduction 1
World Situation 1
Potential Impact Generally 3
Russia's Draft Resolution 4

Information Terrorism and Computer Crimes 6
Introduction 6
Vulnerability of the United States 7
Impact 8
Overhyped? 8
Definitional Issues 9
Computer Crime 9
1. OECD Proposed List of Computer Crimes 11
2. COE Proposed List of Computer Crimes 15
3. Draft Convention on Computer Crime 19
Information Terrorism 27
Jurisdictional Issues 31
Prescriptive 31
1. Universal 31
a. International Law 31
b. Domestic Implementation 33
2. Territorial Jurisdiction 34
a. Subjective 34
(1) The Criminal Act 34
(2) Territorial Limits 35
b. Objective 35
(1) The Act 35
(a) Agency 36
(b) Continuing Act 36
(2) The Intent 38
(3) The effects 38
3. Passive Personality 39
4. Nationality 40
5. Protective Principle 41
6. Consensual 41
7. Concurrent Jurisdiction 43
8. Domestic 44
9. General Considerations 44
a. Mutual Assistance 45

b. Recognition of Judgements 45
c. Extradition 46
d. Evidentiary Problems 46
Enforcement 47
1. Transborder Searches via Electronic Access 49
a. Without Authorization 49
b. Tracing 49
2. Data Collection and Preservation 50
Constitutional Issues 52
First Amendment 52
Fourth Amendment 54
Fifth Amendment 54
Statutory Concerns 56
Privacy 56
Other 58
What Do Existing Treaties Already Cover 58

Conclusion 60

Endnotes 62

FOREWORD

We are pleased to publish this thirtieth-second volume in the *Occasional Paper* series of the US Air Force Institute for National Security Studies (INSS). This paper, along with Occasional Paper 33, Steven Rinaldi's *Sharing the Knowledge: Government-Private Sector Partnerships t0 Enhance Information Security*, address the context surrounding the question of how the U.S. military responds to the cyber threat facing the American military and society today. Rinaldi examines the issues of partnering and sharing sensitive information across private and governmental sectors as a central requirement of a national risk reduction and management effort in the face of the threat of cyber attack. In this paper, Richard Aldrich examines definitional and jurisdictional issues, Constitutional and statutory concerns, and both the necessity and desirability of an international treaty addressing cyberterrorism and computer crime. Together these two papers provide fresh thinking and critical perspective on a security threat arena that increasingly captivates the headlines.

About the Institute

INSS is primarily sponsored by the National Security Policy Division, Nuclear and Counterproliferation Directorate, Headquarters US Air Force (HQ USAF/XONP) and the Dean of the Faculty, USAF Academy. Our other sponsors currently include the Air Staff's Intelligence, Surveillance, and Reconnaissance Directorate (XOI) and the Air Force's 39th Information Operations Squadron; the Secretary of Defense's Office of Net Assessment (OSD/NA); the Defense Threat Reduction Agency (incorporating the sponsorship of the Defense Special Weapons Agency and the On-Site Inspection Agency); the Army Environmental Policy Institute; the Plans Directorate of the United States Space Command; the Air Force long-range plans directorate (XPXP);

and the Nonproliferation Center of the Central Intelligence Agency. The mission of the Institute is "to promote national security research for the Department of Defense within the military academic community, and to support the Air Force national security education program." Its research focuses on the areas of greatest interest to our organizational sponsors: arms control, proliferation, regional studies, Air Force policy, information operations, environmental security, and space policy.

INSS coordinates and focuses outside thinking in various disciplines and across the military services to develop new ideas for defense policy making. To that end, the Institute develops topics, selects researchers from within the military academic community, and administers sponsored research. It also hosts conferences and workshops and facilitates the dissemination of information to a wide range of private and government organizations. INSS provides valuable, cost-effective research to meet the needs of our sponsors. We appreciate your continued interest in INSS and our research products.

JAMES M. SMITH
Director

EXECUTIVE SUMMARY

On the first of October, 1998, the Russian Foreign Minister sent an official request to the Secretary General of the United Nations requesting the world body to look into the appropriateness of establishing international agreements to control the use of "particularly dangerous information weapons as well as to combat information terrorism and criminality, including creation of an international system to monitor the threats related to the security of global information and telecommunications systems."[1] The request was generalized a month later, in response to the concerns of the United States and other western states. As so modified, it was placed on the agenda for the 54th Session of the General Assembly by consensus vote. This paper assesses some of the preliminary legal issues surrounding the establishment of international agreements covering information warfare, information terrorism and cyber crime.

Warfare, terrorism and crime committed with the use of information systems and tools portend an ominous threat to the increasingly information-based economies of the world's leading countries. The United States, with its highly networked infrastructure, is perhaps both the most powerful and the most vulnerable. The Pentagon is expected to suffer about two million information attacks this year alone, and business losses to cyber crime, though difficult to measure precisely, total in the billions of dollars each year. So what would be the relative advantages and disadvantages of international agreements to deal with these burgeoning threats?

The first problem will come in defining the scope of the treaties. Information warfare, information terrorism, and computer crime are all

[1] Informal translation of Russian Foreign Minister's Letter to United Nations Secretary General Kofi Annan as provided by the Policy and

terms that elude facile definitional bounding. In its broadest sense, information warfare includes such time-honored and accepted practices as deception and misdirection, long recognized as legal ruses under the law of war and surely not the proper subjects of treaty limitation. The international community has long decried terrorism even though that community has been unable to agree on what is encompassed by the term. Domestically, terrorism is defined under two separate statutory sections both requiring violence or the threat to or taking of human life for political ends. Such a definition excludes the vast number of information attacks, otherwise denominated as terroristic, which would only result in large-scale financial losses, electrical power grid shutdowns, or mass chaos caused by the manipulation or destruction of information databases. Even the definition of computer crime has been hard to pin down. The Department of Justice has defined it as broadly as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation or prosecution."[2] But certainly as prosecutors and law enforcement investigative units become increasingly technological, computer technology will be employed in the prosecution and/or investigation of virtually any crime.

Other treaties have also been plagued by definitional issues, yet have overcome them. Assuming the international community can overcome the definitional complications, what would a treaty dealing with cyber crime have to offer? First, it would clarify jurisdiction over cyber crimes and information terrorism. While existing treaties and statutes may be capable of pulling select cyber crimes within their ambit, there is little uniform treatment for cyber crimes. Thus, a new cyber crime treaty could help provide the basis for criminalizing the vast array

---

Issues Group of the Central Intelligence Agency.

[2] NATIONAL INSTITUTE OF JUSTICE, U.S. DEP'T OF JUSTICE, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCE MANUAL 2 (1989).

of cyber offenses that do not cleanly fit within traditional crimes. It would also aid extraditions by overcoming the dual criminality problem. Even more importantly, a new treaty could establish agreed principles of enforcement jurisdiction to enable law enforcement to more quickly, easily, and legally obtain the evidence necessary for the prosecution of cyber crimes and information terrorism.