

### ENDNOTES

- <sup>1</sup> P.J. Baines, "Prospects for 'Non-Offensive' Defenses in Space" in James Clay Moltz, ed., *New Challenges in Missile Proliferation, Missile Defence and Space Security*, Center for Nonproliferation Studies, Monterey, California, Occasional Paper no. 12, p.31.
- <sup>2</sup> S. Zhdakaev, et. al., "Dumb Bombs," *Izvestia*, Moscow, 25 March 2003, p.1.
- <sup>3</sup> W.E. Burrows, *Deep Black Space Espionage and National Security*, (Random House: New York, 1986), p.282.
- <sup>4</sup> Government of Canada, Department of National Defence, OCIPEP Daily Brief Number: DOB02-071, Ottawa, 30 May 2002.
- <sup>5</sup> "Information Security - Computer Hacker Information available on the Internet," General Accounting Office, Senate Hearing Report, 5 June 1996. Available at <http://www.fas.org/irp/gao/aimd-96-108.htm>.
- <sup>6</sup> W.J. Larson, and J.R. Wertz, eds., *Space Mission Design and Analysis*, 2nd ed., (Kluwer Academic Publishers: Dordrecht, 1992), p.215-228.
- <sup>7</sup> J. Davis and R. S. Murch, "High Altitude Nuclear Detonations (HAND) Against Low Earth Orbit Satellites (HALEOS)," Defense Threat Reduction Agency, April 2001, presentation available at [www.fas.org](http://www.fas.org).
- <sup>8</sup> J. Davis and R. S. Murch, "High Altitude Nuclear Detonations (HAND) Against Low Earth Orbit Satellites (HALEOS)," Defense Threat Reduction Agency, April 2001, presentation available at [www.fas.org](http://www.fas.org).
- <sup>9</sup> J. Cirincione, "The Declining Ballistic Missile Threat," Testimony of Project Director Joseph Cirincione before a special meeting of the Danish Parliament - The Folketing, 24 April 2003. Available at [www.ceip.org](http://www.ceip.org).
- <sup>10</sup> "Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques," Geneva, 18 May 1977.
- <sup>11</sup> "Anti-Satellite Weapons, Countermeasures, and Arms Control," US Congress, Office of Technology Assessment, OTA-ISC-28, Washington, D.C., September 1985.
- <sup>12</sup> M.E. Polites, "An Assessment of the Technology of Automated Rendezvous and Capture in Space," NASA/TRP-1998-208528, Marshall Space Flight Center, NASA, July 1998.
- <sup>13</sup> US Department of Defense, "Annual Report to Congress on the Military Capability of the Peoples Republic of China," United States, Department of Defense, Washington D.C., June 2000. Available at <http://www.defenselink.mil/news/Jun2000/china06222000.htm>.
- <sup>14</sup> S. Komarow, "Army scores a hit on satellite in test of laser," *USA Today*, 21 October 1997, p.A6.
- <sup>15</sup> "Pentagon Beams Over Laser Test: US Wants to Determine Vulnerability of Satellites," *CNN*, 20 October 1997. Available at <http://www.cnn.com/US/9710/20/pentagon.laser/>.
- <sup>16</sup> S. Komarow, "Army scores a hit on satellite in test of laser," *USA Today*, 21 October 1997, p.A6.
- <sup>17</sup> "National Space Policy," US White House Fact Sheet, 19 September 1996.
- <sup>18</sup> "Strategic Master Plan FY04 and Beyond," United States, Air Force Space Command, Peterson Air Force Base, Colorado, 5 November 2002. Available at <http://www.cdi.org/news/space-security/afspc-strategic-master-plan-04-beyond.pdf>.
- <sup>19</sup> "Annual Report on the Military Power of the People's Republic of China," United States, Department of Defense, Washington, D.C., 28 July 2003. Available at <http://www.defenselink.mil/pubs/20030730chinaex.pdf>.

## I-11 Space Systems Negation

them. Spoofing attacks that seek to gain unauthorized access to a space system by emulating an authentic user could permit an intruder to disrupt normal satellite operations.<sup>3</sup> Given the current state of telemetry and spacecraft reliability, an operator might never know whether such an anomaly was an ordinary onboard glitch or the work of a hostile actor.

Cyber attacks are becoming more commonplace. On 28 May 2002 the grassroots Netstrike Against NATO campaign launched a distributed denial-of-service attack against the main website of NATO, coinciding with a meeting of its leaders in Italy.<sup>4</sup> While the US Department of Defense's computer systems have been attacked almost every day for years (estimated at 250,000 times in 1996), the real number of these attacks is difficult to assess because such a small number are actually detected.<sup>5</sup> While the military space assets of the most advanced space-faring states are relatively well protected, not all space security actors enjoy this level of protection, making this type of space negation capability an attractive and relatively low-cost option for many states.

**Robotic Manipulation.** Satellites are relatively fragile and ungainly systems; they often require devices dedicated to keeping them pointed in the right orientation to ensure their proper operation. Consequently, some satellites could be 'tipped over' by a robotic servicing device from which states they might never recover. Thus, in-orbit robotic manipulators represent a potential space negation capability. Concerns about this capability were expressed by the former Soviet Union over the development of the US space shuttle and its Canadian shuttle remote manipulator system, more commonly known as the Canadarm (see Figure 11-5). However, the likelihood of robotic manipulation systems being used as a space negation capability is remote as it would represent the use of very expensive and complex systems to allow missions that could otherwise be accomplished by less expensive means. This technology is assessed to be limited to the United States, the European Union, Russia, Japan, and Canada.

### Permanent or Irreversible Space Negation - Degradation and Destruction

Beyond temporary space system negation efforts, negation may also be undertaken through the application of force to degrade or actually destroy the ground or space segments of an adversary's space systems. Terrestrial satellite control and launch facilities are vulnerable to a wide range of military attacks that could degrade or completely destroy essential components of an actor's space systems or their access to space. Indeed, this approach is widely assessed to be the most cost effective and readily achievable space negation option for most actors. However, attacks against control stations would risk the creation of collateral space debris because satellites without effective ground stations would not receive orbit control or space debris mitigation commands.



Figure 11-4  
StoptheNATO.org's Netstrike  
Against NATO campaign.

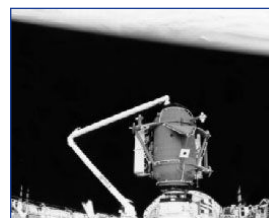


Figure 11-5  
Canadarm being used to  
install the shuttle docking  
port on Mir.



# SPACE SECURITY

---

2003



THE  
**EISENHOWER**  
INSTITUTE

# SPACE SECURITY

---

# 2003

THE  

---

**EISENHOWER**  

---

INSTITUTE

THE  
**EISENHOWER**  
INSTITUTE

Published in Washington, DC

© The Eisenhower Institute 2004

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, without the prior permission in writing of The Eisenhower Institute.

ISBN 0-920231-36-5

Printed in Toronto  
by Northview Press Ltd.