SPACE AND CYBER: A CRITICAL LEGAL NEXUS

Deborah Housen-Couriel
Interdisciplinary Cyber Research Center, Tel Aviv University
How an international treaty signed 50 years ago became the backbone for space law

Happy anniversary, Outer Space Treaty

by Loren Grush | @lorengrush | Jan 27, 2017, 11:14am EST

The signing of the Outer Space Treaty. | United Nations

Fifty years ago today, the United States, the Soviet Union, and the United Kingdom opened a treaty for signature that would become the backbone for international space law. It was a United Nations-approved agreement called the Outer Space Treaty, and
FOCUS ON A CRITICAL LEGAL NEXUS

OUTER SPACE
ABOVE EARTH’S ATMOSPHERE

SATellite COMMUnications

Cyberspace
Computers, Data, Transmission Infrastructures, People
The hacks of the Joint Polar Satellite System took place between August 2014 and August 2015, according to the report published by the Government Accountability Office. The incidents were classified as ranging from medium to high severity, and included "hostile probes, improper usage, unauthorized access, password sharing and other IT-related security concerns."
HOSTILE CYBER OPERATIONS AGAINST JOINT POLAR SAT SYSTEM
VULNERABILITY THROUGHOUT THE SATELLITE LIFESPAN

- Pre-launch and launch
- TT&C
- Physical destruction or disabling
- Disruption of transmissions—full taxonomy
- End-of-life events, “crashes”
TYPES OF CYBER-ENABLED DISRUPTIONS TO SAT COMM (via EM SPECTRUM)

- JAMMING
- MORPHING
- HIJACKING TT&C >> COLLISION
- ‘GRILLING’
- SIGNAL RE-ROUTING
NOT NEW / UNIQUE

- 1997 UNTIL PRESENT - TURLA INTERNET CONNECTION HACKING GROUP
- 2007-8 LANDSAT AND TERRA AM-1 HACKS
- SUMMER 2015 - ALLEGED INTERference WITH GLOBALSTAR’S ASSET-TRACKING SYSTEMS (+ SOUTH KOREAN FISHERMEN)
- ONGOING NASA HACKS – GROUND SEGMENT
HIGH-RISK SCENARIOS

“Because of the criticality of satellite data to weather forecasting, the possibility of a satellite data gap, and the potential impact of a gap on the health and safety of the U.S. population and economy, we added this issue to GAO’s High Risk List in 2013 and it remained on the list in 2015.” – 2017 update due
EXTRAPOLATING > LOSS-OF-LIFE SCENARIOS DUE TO SAT DEPENDENCY
GROWING CRITICALITY AND URGENCY AT THE NEXUS

SPACE LAW (TREATIES, NAT’L LAWS)

- ‘PEACEFUL USE’ ISSUES
- LIABILITY ISSUES
- STATE PRACTICE NOT TRANSPARENT

CYBER LAW (EMERGING and ITU TELECOM)

- USE OF FORCE / SD
- CONCEPTUAL / NORMATIVE ISSUES
- ROLE OF PRIVATE CORPORATIONS

SATELLITE CONTROL OF CRITICAL INFRASTRUCTURE >> VULNERABILITIES
HOW IS THE INTERNATIONAL LEGAL COMMUNITY MEETING THIS CHALLENGE AT THE NEXUS OF THE TWO REGIMES?

BEGINNING TO ENGAGE WITH THE INTERSECTION OF SPACE + CYBER RULES
Sixty-eighth session
Item 99 (c) of the provisional agenda**
General and complete disarmament: transparency and confidence-building measures in outer space activities

Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities

Note by the Secretary-General

The Secretary-General has the honour to transmit herewith the report of the Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities. The Group was established pursuant to General Assembly resolution 65/68.

Seventieth session
Item 93 of the provisional agenda*
Developments in the field of information and telecommunications in the context of international security

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Note by the Secretary-General

The Secretary-General has the honour to transmit herewith the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. The Group was established pursuant to paragraph 4 of General Assembly resolution 68/243.
TALLINN MANUAL 2.0
ON THE INTERNATIONAL LAW
APPLICABLE TO CYBER OPERATIONS

Prepared by the International Groups of Experts
at the Invitation of the NATO Cooperative
Cyber Defence Centre of Excellence

2016-2017: Academic and Policy Inputs
CONSENSUS:

THIS IS NOT ONLY A PROCEDURAL OR GOVERNANCE CHALLENGE...

IT’S A SUBSTANTIVE ONE.
HARMFUL DISRUPTION VULNERABILITIES: CYBER ATTACKS ON SATELLITE COMMS CAN CONSTITUTE PROHIBITED USES OF FORCE > SELF-DEFENSE
The necessary and critical conversation between these two legal regimes has begun – needs to be deepened at all levels.

There's a key role for private companies that has not yet been explored.
“DE-SILO”

THANK YOU.

deborah@cyberregestrategies.com
EXTRA SLIDES
GGE SPACE 2013

SHANGHAI PPWT
June 2014 (rev)

EU CODE OF CONDUCT
March 2014 (rev)

Other initiatives:

GGE CYBER 2015

SHANGHAI CODE OF CONDUCT
January 2015 (rev)

EU / CoE
Budapest Convention, 2001

Other initiatives:
Tallinn Manuals 1 & 2
OST Article IV

OST establishes “peaceful use” principle, yet the compromise arrangements in fact permit military activity

- division into earth orbit, moon and celestial bodies, outer space
- military activity, including ASAT, prohibited on moon and cb’s
- in outer space illegal aggression and WMD forbidden
- Civilian – military research permitted
- only limited disarmament
NEXT STEPS: WHAT’S TO BE DONE AND WHO SHOULD DO IT?

CONSIDER HOW TO MOVE JOINTLY FROM TCBMs TO SUBSTANTIVE NORMS

AS NORMATIVE WORK IS ONGOING – IDENTIFY AND SHARE BEST PRACTICES (ENCRYPTION)

MERGE WORK PROCESSES OF RELEVANT INTER-GOV’T INITIATIVES (CO-COMMITTEES, CONFERENCES)

CRITICAL CHALLENGES FOR LEGAL AND POLICY COMMUNITIES