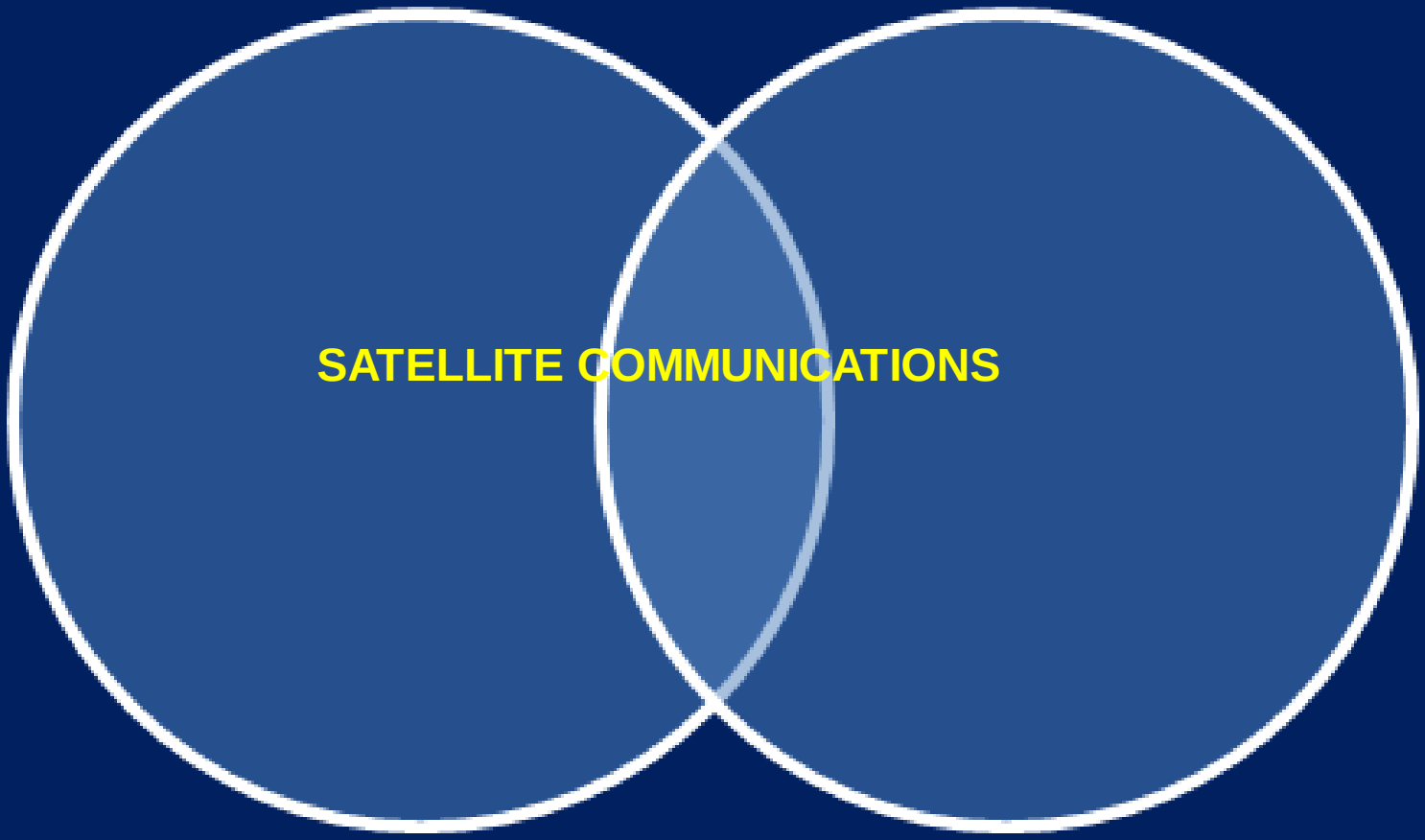
10TH UNITED NATIONS WORKSHOP ON SPACE LAW
September 5-8, 2016

SPACE SECURITY AND CYBERSECURITY:

INTERSECTING CHALLENGES

Deborah Housen-Couriel
Interdisciplinary Cyber Research Center, Tel Aviv University

FOCUS ON A CRITICAL NEXUS



WASHINGTON Examiner

GAO: Hackers penetrating national weather satellites

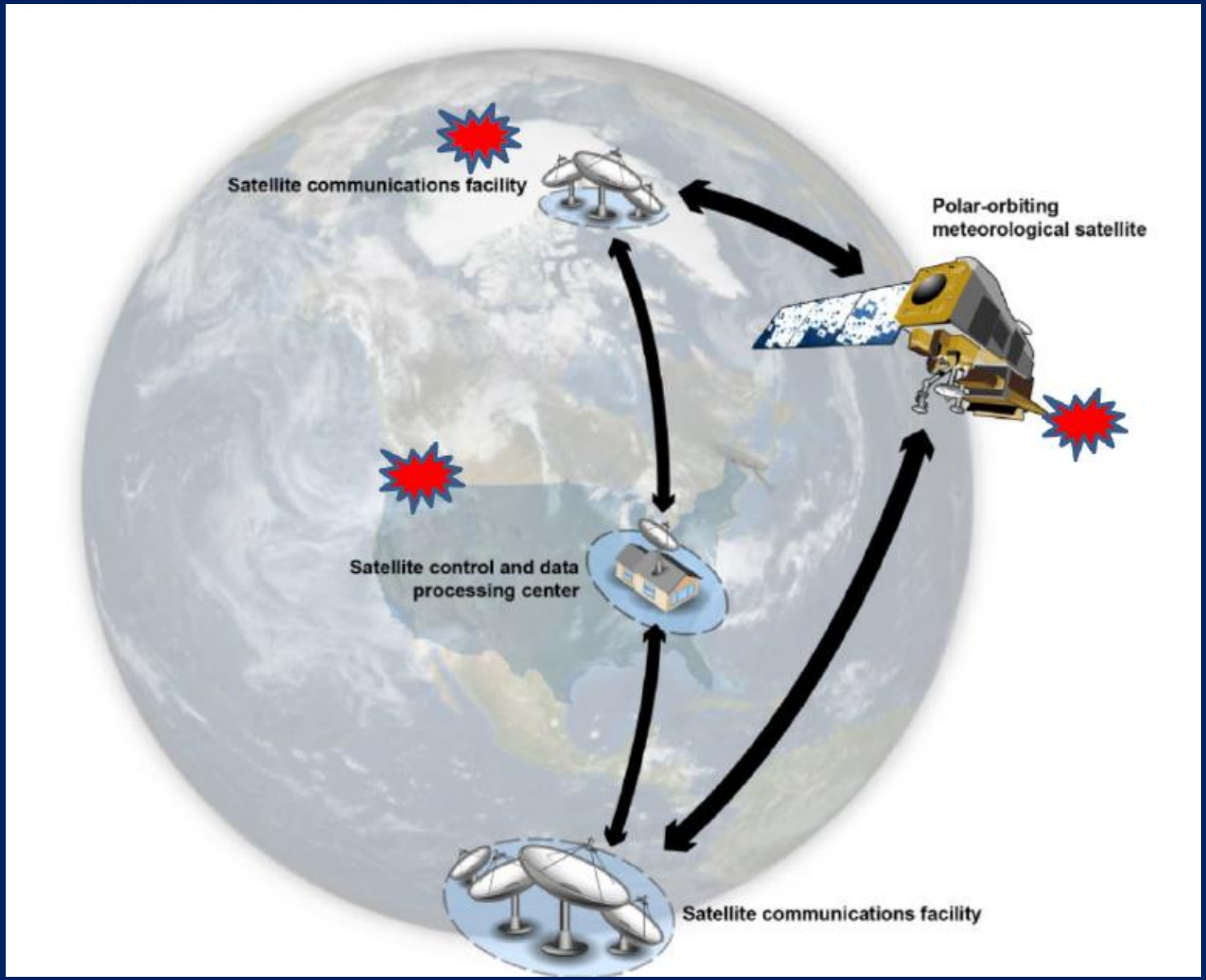
By RUDY TAKALA (@RUDYTAKALA) • 5/19/16 11:40 AM

U.S. weather satellites were breached 10 times over the course of a year, according to a congressional agency.

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

SPACE / GROUND SEGMENTS



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

TYPES OF CYBER-ENABLED DISRUPTIONS TO SAT COMM (via EM SPECTRUM)

JAMMING

MORPHING

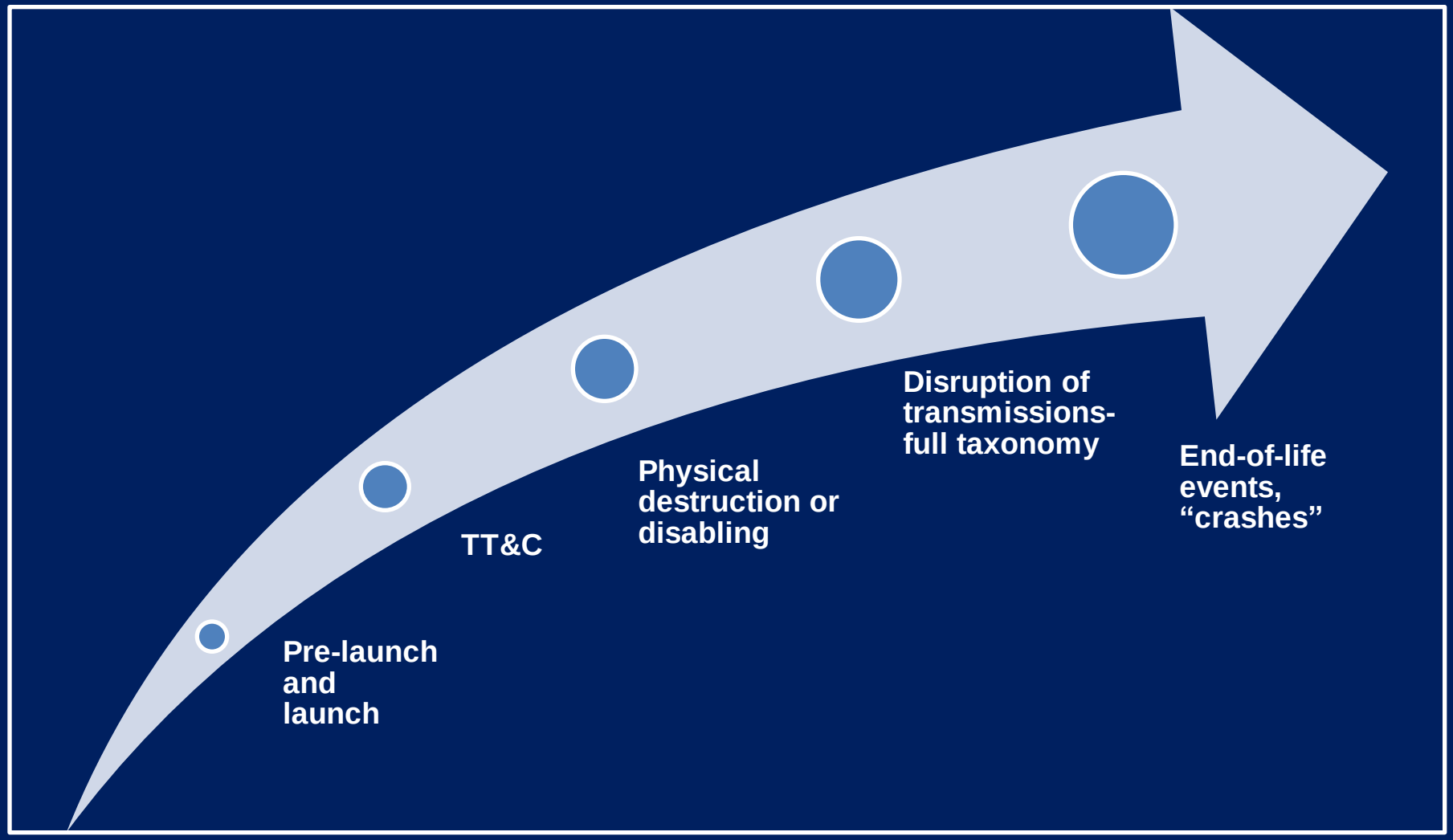
HIJACKING
TT&C >>
COLLISION

'GRILLING'

TURLA-TYPE

SIGNAL RE-ROUTING

VULNERABILITY THROUGHOUT THE SATELLITE LIFESPAN

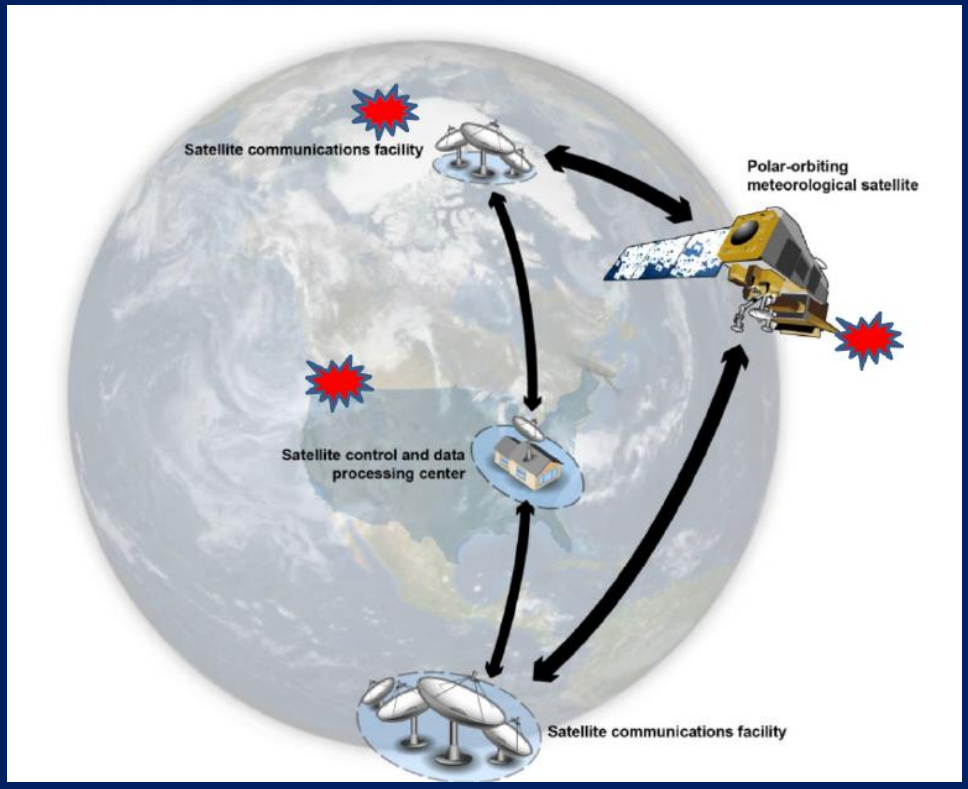


WORKING DEFINITION: HOSTILE DISRUPTION OF SATCOMM

Physical, cyber-enabled and hybrid disturbance to satellites and satellite communications, originating in a hostile intent to disrupt, damage or otherwise disturb their uninterrupted operation.

- **"harmful interference" under ITU Constitution + RR**
  - **also under Article IX of the OST [query]**

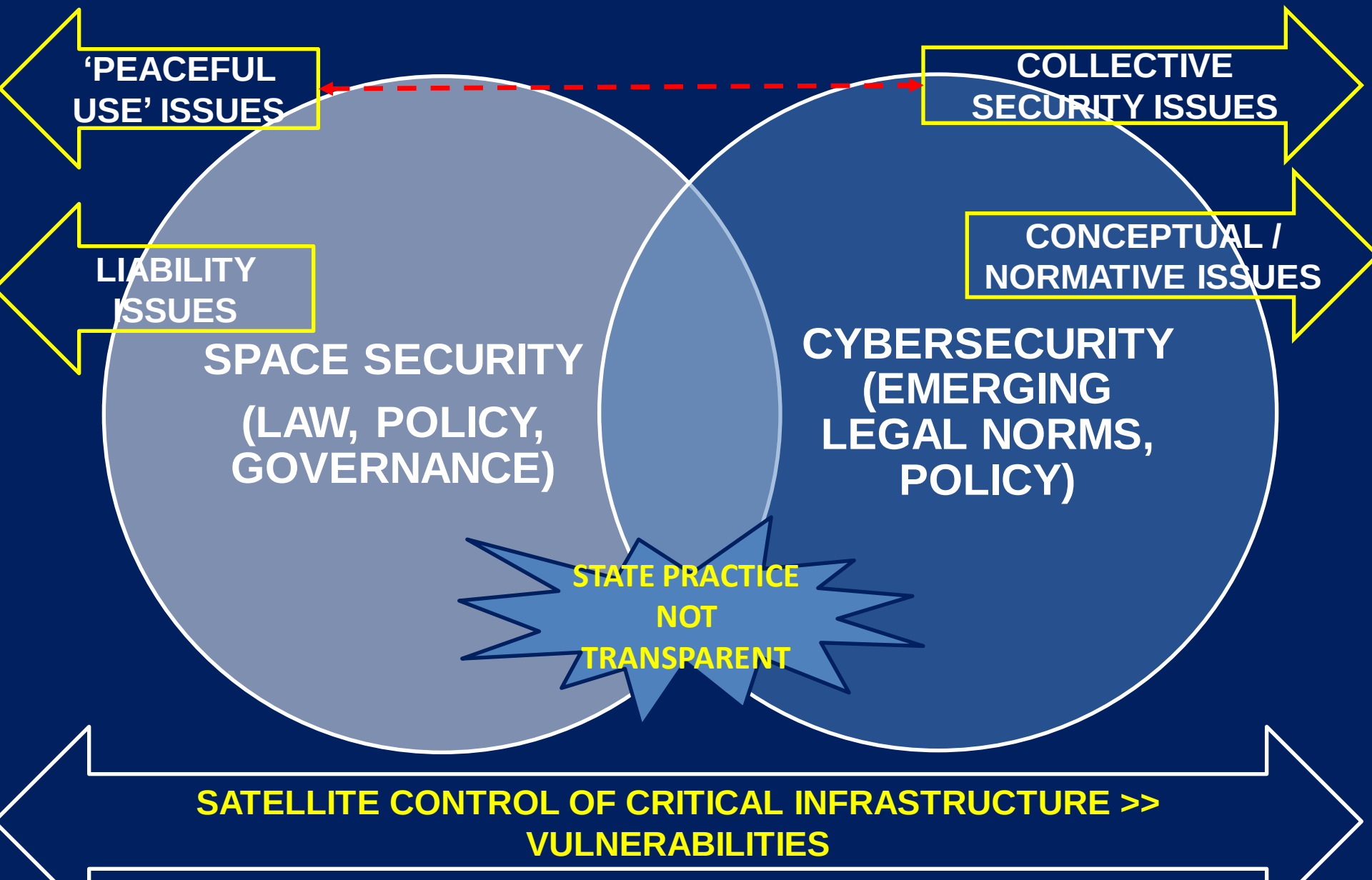
THESE ARE HIGH-RISK SCENARIOS



"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."

EXTRAPOLATING > LOSS-OF-LIFE SCENARIOS

THE GROWING CRITICALITY AND URGENCY OF THE PROBLEM AT THE NEXUS



4 COMMON CORE CHALLENGES

1. • CHANGING ACTORS / STAKEHOLDERS
2. • DUAL-USE TECHNOLOGIES
3. • LACK OF NAT'L POLICY TRANSPARENCY
4. • LACK OF EFFECTIVE INTN'L COOPERATION

HOW IS THE INTERNATIONAL LEGAL COMMUNITY MEETING THIS CHALLENGE AT THE NEXUS OF THE TWO REGIMES?

SPACE + CYBER GGE's

2013

United Nations A/68/189*

General Assembly

Distr.: General
29 July 2013

Original: English

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.

2015

United Nations A/70/174

General Assembly

Distr.: General
22 July 2015

Original: English

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.

GGE SPACE 2013

- SHANGHAI PPWT June 2014 (rev)
- EU CODE OF CONDUCT March 2014 (rev)
- Other initiatives: Canada Proposal, CD, June 2009; ITU-R; UNGA 69/32, 2014; Working Group on 5 Treaties, 2016

GGE CYBER 2015

- SHANGHAI CODE OF CONDUCT January 2015 (rev)
- EU / CoE Network Security Directive, 2013
- Budapest Convention, 2001
- Other initiatives: Tallinn Manuals 1 & 2

THIS IS NOT ONLY A PROCEDURAL OR GOVERNANCE CHALLENGE…

IT'S A SUBSTANTIVE ONE.

BRIEF CASE STUDY

AT WHAT THRESHOLDS DO HOSTILE SATCOMM DISRUPTIONS

AN ILLEGAL USE OF FORCE IN SPACE AND CYBERSPACE?

APPLICABILITY OF INTERNATIONAL LAW IN CYBERSPACE

- We affirm that international law, including the United Nations Charter, is applicable in cyberspace.
- We affirm that under some circumstances, cyber activities could amount to the use of force or an armed attack within the meaning of the United Nations Charter and customary international law. We also recognize that states may exercise their inherent right of individual or collective self-defense as recognized in Article 51 of the United Nations Charter and in accordance with international law, including international humanitarian law, in response to an armed attack through cyberspace.

G7 / G20 PRINCIPLES AND ACTIONS ON CYBER, 2016

-- NATO, ARTICLE 5
-- US, UK, NL

ALL MEMBERS SHALL REFRAIN …FROM THE THREAT OR USE OF FORCE AGAINST THE TERRITORIAL INTEGRITY OR POLITICAL INDEPENDENCE OF ANY STATE...

UN 2(4)

NOTHING IN THE PRESENT CHARTER SHALL IMPAIR THE INHERENT RIGHT OF …SELF-DEFENSE IF AN ARMED ATTACK OCCURS AGAINST A MEMBER OF THE UN...

UN 51

"No state can be expected to await an initial attack which…may well destroy the state's capacity for further resistance and so jeopardize its very existence."

Derek Bowett, 1958

"All the News That's Fit to Print"

The New York Times.

LATE CITY EDITION

VOL. CXII...No. 38,258. NEW YORK, TUESDAY, OCTOBER 23, 1962. FIVE CENTS

U.S. IMPOSES ARMS BLOCKADE ON CUBA ON FINDING OFFENSIVE-MISSILE SITES; KENNEDY READY FOR SOVIET SHOWDOWN

U. S. JUDGES GIVEN POWER TO REQUIRE VOTE FOR NEGROES

Chinese Open New Front; Use Tanks Against Indians

Nehru Warns of Peril to Independence —Reds Attack Near Burmese Border and Press Two Other Drives

SHIPS MUST STOP

Other Action Planned If Big Rockets Are Not Dismantled

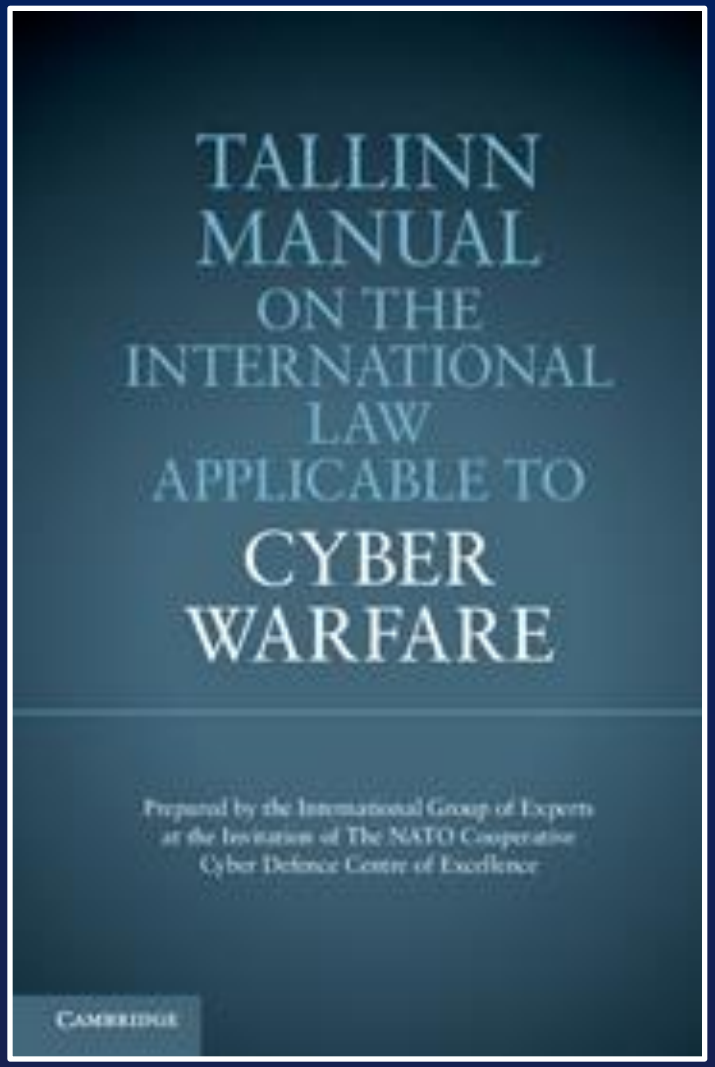
PRESIDENT GRAVE

Asserts Russians Lied and Put Hemisphere in Great Danger

ANTICIPATORY / PRE-EMPTIVE SELF-DEFENCE

2013

- LEADING EXPERT AUTHORITIES
- NOT STATES (FOR GOOD REASON)
- **INTERNATIONAL LAW AND COLLECTIVE SECURITY APPLY**
- STATES' DE FACTO ACKNOWLEDGEMENT



RULE 30: “CYBER ATTACK”

A CYBER ATTACK IS A CYBER OPERATION, WHETHER OFFENSIVE OR DEFENSIVE, THAT IS REASONABLY EXPECTED TO CAUSE INJURY OR DEATH TO PERSONS OR DAMAGE OR DESTRUCTION TO **OBJECTS**.

RULE 11: “USE OF FORCE”

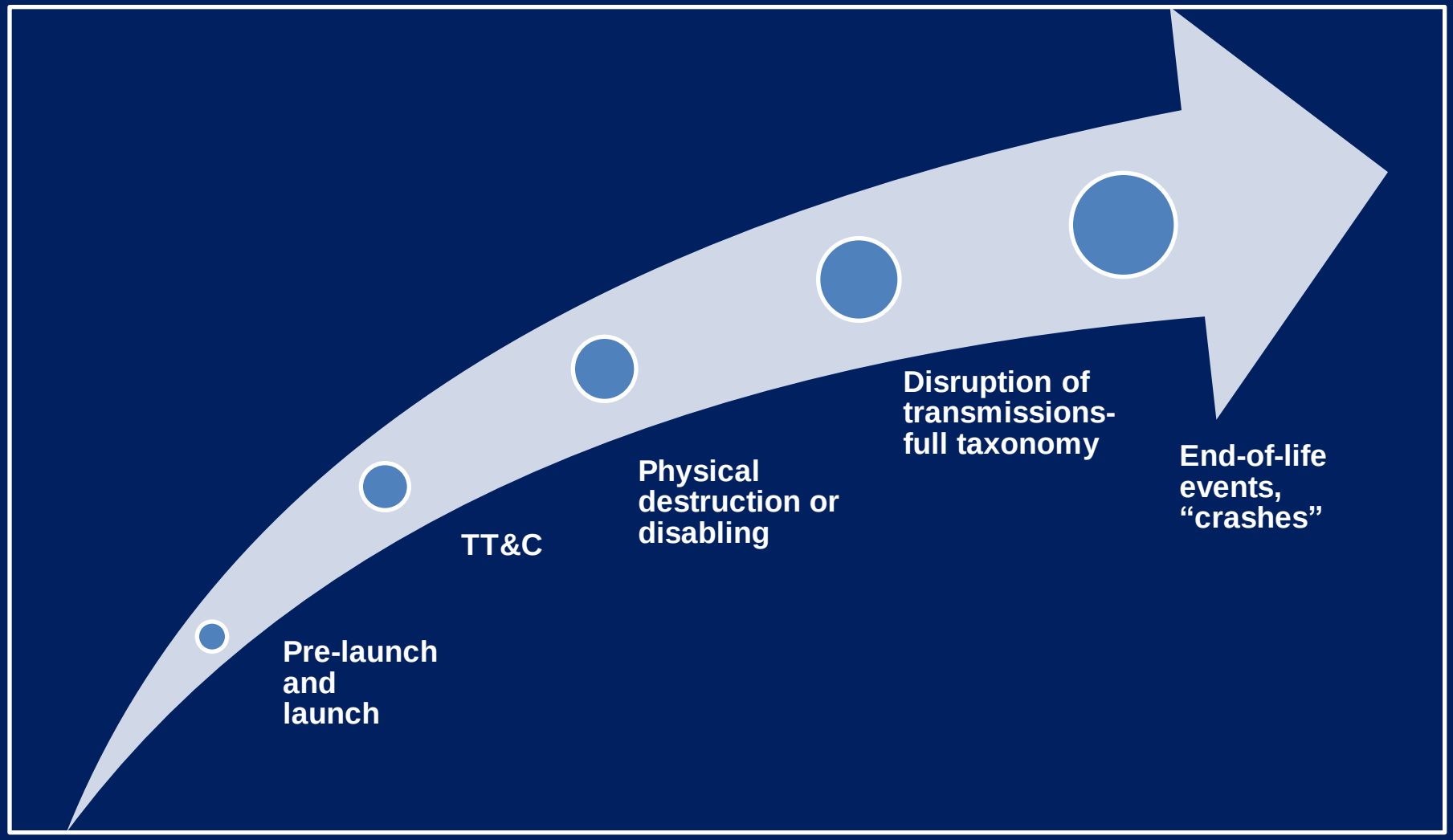
A CYBER OPERATION CONSTITUTES A USE OF FORCE WHEN ITS SCALE AND EFFECTS ARE COMPARABLE TO NON-CYBER OPERATIONS RISING TO THE LEVEL OF A USE OF FORCE.

(ICJ NICARAGUA 1986)

- A decision as to when a cyber attack would lead to the invocation of **Article 5** would be taken…on a case-by-case basis.

- Cyber attacks … could be as harmful to modern societies as a conventional attack … **cyber defence is part of NATO's core task** of collective defence.

HARMFUL DISRUPTION VULNERABILITIES: CYBER ATTACKS ON SATELLITE COMMS CAN CONSTITUTE PROHIBITED USES OF FORCE



SUMMING UP

- **Hostile disturbances to satellite transmissions constitute real threats and challenges, with significant ramifications for collective security.**
- **These challenges intersect because satellite communications are cyber operations.**
- **Beyond operative and governance issues, there are important normative overlaps.**
- **While there's some intergov't progress re admin measures – TCBMs, BPs (GGE's)…**

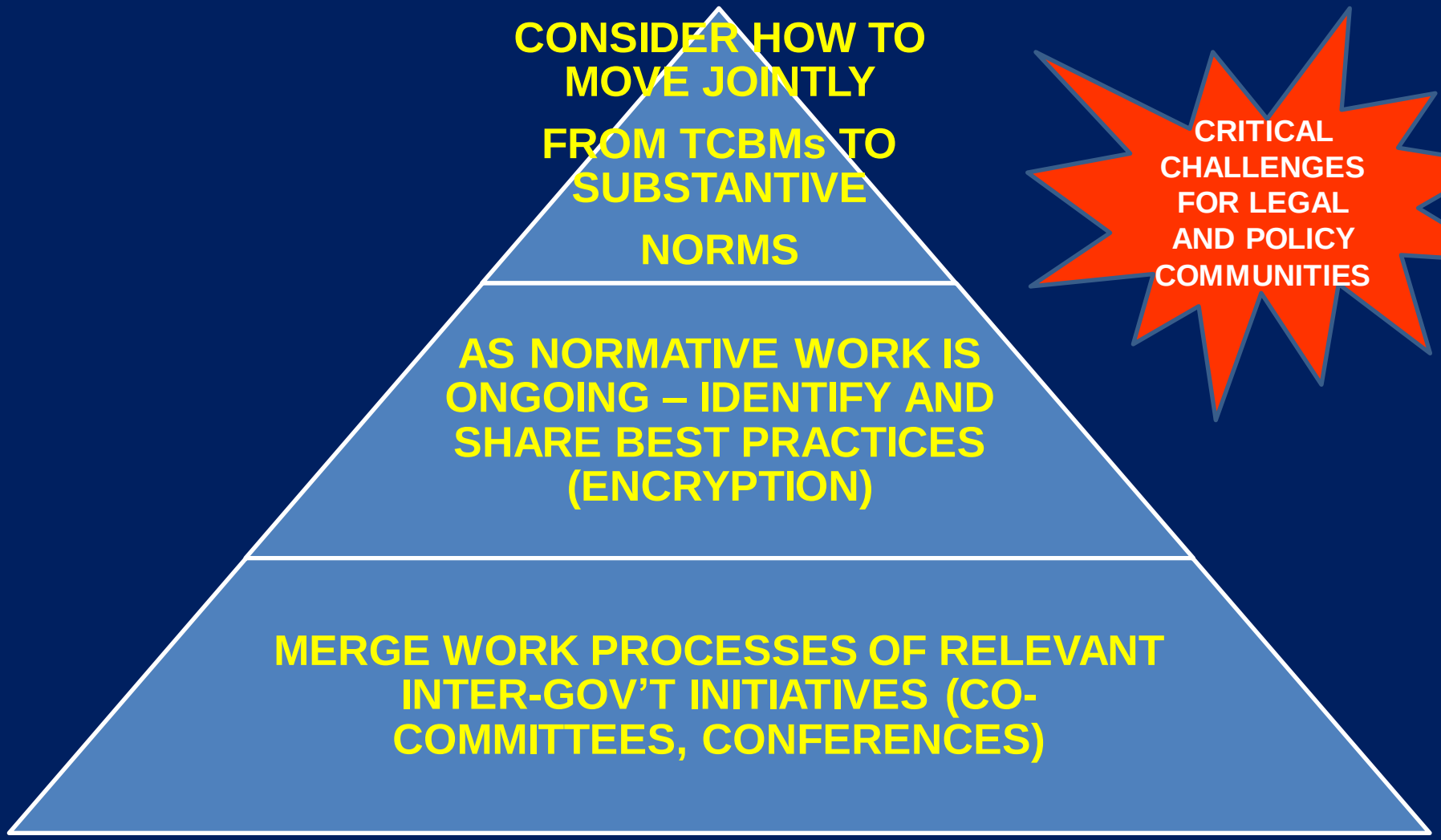
1

- **Insufficient awareness of the operational and normative overlaps**

2

- **The necessary and critical conversation between these 2 legal regimes has yet to begin**

NEXT STEPS: WHAT'S TO BE DONE AND WHO SHOULD DO IT?



“DE-SILO”

THANK YOU.

deborah@cyberregstrategies.com