The Cyber Sea:
Information Security and National Defense

Dr. Paul Losiewicz
ONR Global
Regional S&T Engagement Office
Prague, Czech Republic

The Goal of the Talk

Scientists wanting to understand and mitigate cyber threats to:

a) international stability and

b) national security

We will use the Analogical Method:

A) **Maritime Law as a starting point for discussing Cyberspace Law – ADM James Stavridis, SACEUR**

B) **Cyberspace Law as logical end point under the Laws of War – Dr. R.M. Yusupov**, Director of St.Petersburg Institute for Informatics and Automation of RAS (SPIIRAS)

Cyberspace - the Outlaw Sea

• **International Stability**: countering criminal activity and promoting safe commerce.

• **The Nautical Analogy** – Cooperative sharing of the High Seas, the 1980s Law of the Sea treaty, the largest negotiating project in the history of mankind took ten years to negotiate.

• **The Stavridis Assertion** – "Think about the cyber sea and how you can help tame it. Because it is still an outlaw sea…..We must do that internationally, interagency, private/public, and we've got to do it by strategically connecting.

SACEUR ADDRESS TO
ARMED FORCES COMMUNICATIONS AND ELECTRONICS ASSOCIATION
SAN DIEGO, 2 FEBRUARY 2010

Consider Cyberspace and the *Threat* of War

- A new addendum to Clausewitz' *On War?* What are the economic and social impacts of cyber war on national interests?
- Cyber war -The Clausewitzian pursuit of national policy by other means?
- Historically, Limited *w*ar, assumed by the Principle of Proportionality, *has been moderated* by a credible threat of "total war", which leads us to:
- **The Yusupov Principle**: "But security can not always be guaranteed by protection only. It also requires standardized behavior and objects, interaction rules, high-level professional training of staff, faultless technical specifications, and the reliability of all the different objects that IS [Information Security] functions guarantee. The case is similar to strike-back nuclear weapons which are necessary as a powerful means of *deterring potential attackers* from using this type of weapon.

Science and National Security

translated by Dr. M. Mayskaya and Dr. B. Losiewicz

Both Analogies Consistent and Useful, with Caveats

• **The Stavridis Assertion** is fully consistent with the civilian side of the Clauswiztian continuum of National Means…

- But, can we afford 10 years of international negotiation? Global Warming Summit a case in point …
- Are any other unilateral or bilateral approaches effective?
- Do we have the scientific tools and know-how to make the determination of *when* the Yusupov Principle comes into effect?

• **The Yusupov Principle** has ***stood the test of time*** with respect to deterrence in the nuclear arena…

- But, do we take offensive cyber warfare seriously enough for it to be an effective deterrent?
- Does the analogy fail in the face of the asymmetries in Cyber capabilities?
- Is Cyber non-proliferation a realistic possibility?
- Do we have the scientific tools and know-how to engage in limited Offensive Cyber Operations?

What Role Government R&D?

Scientific Tools and Know-How - technical challenges include:

- Detailed understanding of complex adaptive systems
- Formal methods to enhance software and system reliability
- Models and performance metrics for complex networks
- Detailed understanding of the impact of social networking on national level policy, strategy, and information operations
- Understand the impact of decentralized control mechanisms (e.g. BOT armies) on command and control strategies
- Understand and address the growing reliance by governments and militaries on third party hardware and software components.

LASTLY – International Policy must realistically reflect capability, which is NOT an R&D issue