Cyber Challenge
–
a skeptic's view

jozef.vyskoc@cepolicy.org

Seems we have naming problems

Obvious, but worth to remind

Language of marketing is good to attract attention and incite emotions (perfect to sell something to the public or politicians) but such features makes it unsuitable for scholarly discussions.

In other words – do we really need to use the term cyber **war**?

Obvious, but worth to remind

Wrong selection of a concept at the beginning may be the real reason for later problems

Example: “war” involves weapons, attacks, casualties, heroes, ... consequently using the term “cyber war” results in anticipation of existence of cyber-weapons, cyber-attacks, cyber-casualties, cyber-heroes, ... and call for (and problems with) explanation of their meaning

Risks of talking cyber-something without common understanding of the terms

- **building something on an uncertain, shaky grounds**
- **possible waste of time and/or other resources (by missing what is really important)**

Example (possible waste of time)

Do we really need solution for attribution problem (in cyberspace)?

Answer: it depends ... not necessary for cyber defense purpose, important if revenge/punishment is sought ... thus please state explicitly your priorities

We need basis for discussion, i.e.

- **clear, common understanding of key terms**
- **“axioms” – statements catching important peculiarities of cyberspace that need to be taken into account**

... also debunking some myths may be useful

Example – axiom on illusion of control

When it comes to control of a computer system (part of cyberspace)

1.it is possible to have full physical control over it, but

2.if the system is switched on with software running and accepting input data, no one, not even owner, has warranted full control over its behavior