CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

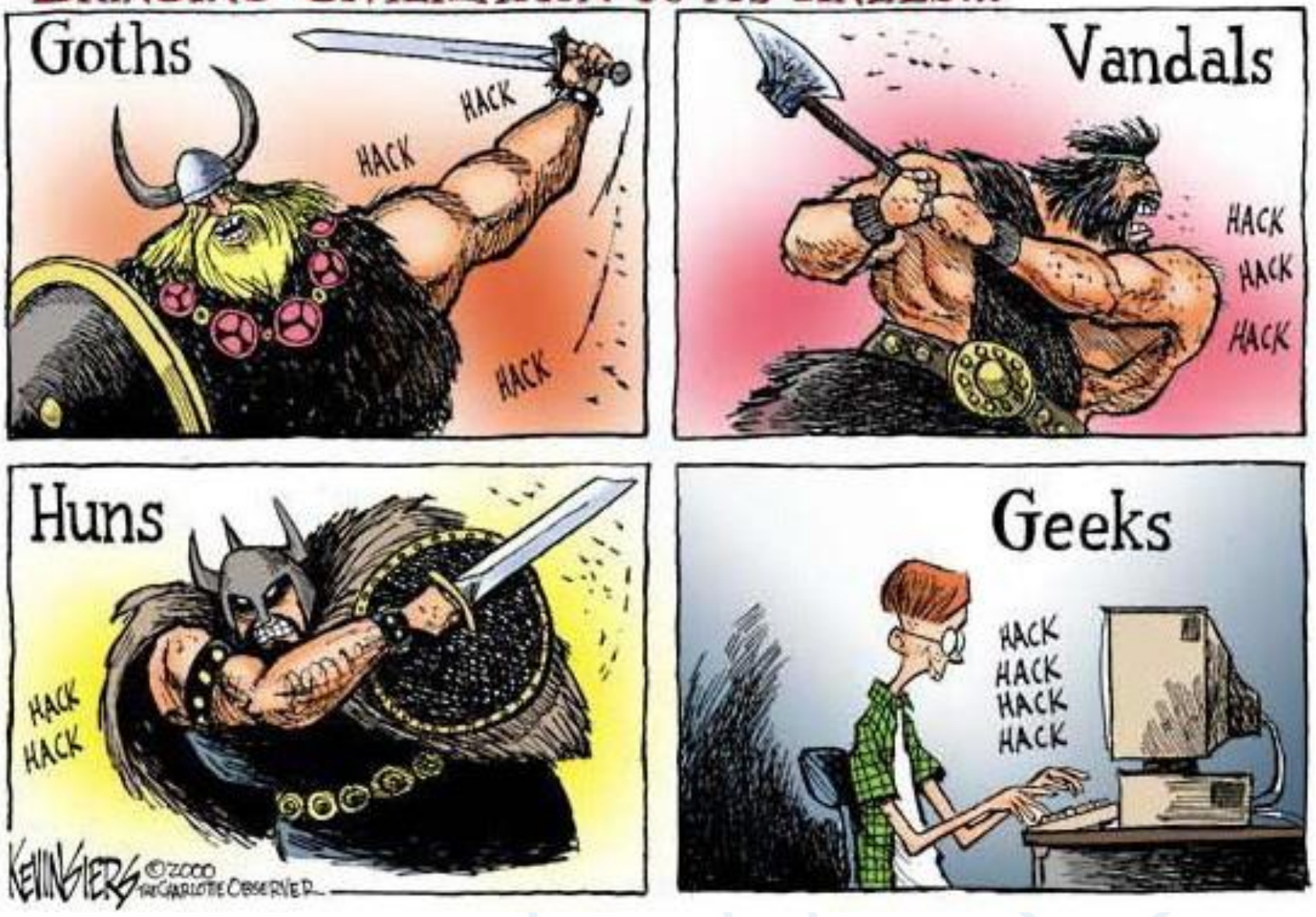
Sponsoring nations

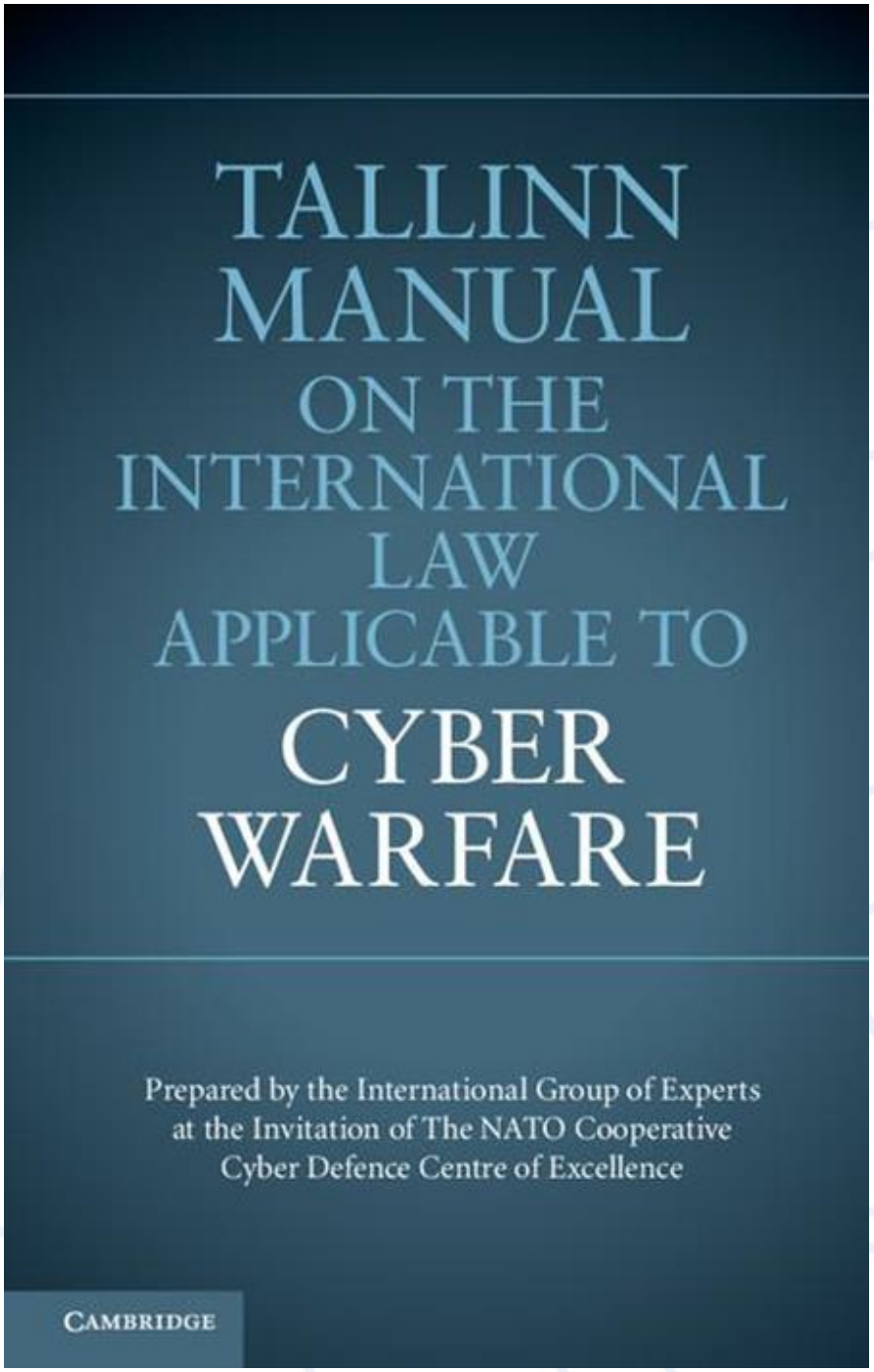
Contributing participants

LOCKED SHIELDS

CROSSED SWORDS

BRINGING CIVILIZATION TO ITS KNEES...




TALLINN
MANUAL
ON THE
INTERNATIONAL
LAW
APPLICABLE TO
CYBER
WARFARE
Prepared by the International Group of Experts
at the Invitation of The NATO Cooperative
Cyber Defence Centre of Excellence
CAMBRIDGE


THE WEAPONS AT THEIR FINGERTIPS
10,000 BC
10 BC
1500 AD
1700 AD
1910 AD
2010 AD
SURFACE-TO AIR
TODAY
DRONE STRIKE
CYBER-ATTACK
KAL

International Conference on Cyber Conflict

TALLINN, ESTONIA


Q:
WHAT WILL THE WARRIOR-GUARDIAN OF THE FUTURE LOOK LIKE?
YO! DUDE.. BACK HERE
CYBER SECURITY

The Information Sphere Domain
Increasing Understanding and Cooperation

Dr. PATRICK, D. ALLEN and Dennis P. GILBERT, Jr
Johns Hopkins University, Applied Physics Lab
Booz Allen Hamilton

Abstract. Recent discussions regarding the emerging field of cyber warfare have focused on the term "cyberspace," and have included cyberspace as being considered its own war fighting domain, much like air, land, sea, and space. In this stage of the Information Age, the international community is grappling with whether it needs to define this information realm as a domain, similar to the air, land, sea, and outer space domains that already exist. History shows that there is always an advantage in a conflict to the side that *understands and operates* within a domain better than the opponent. In this paper, the authors propose a definition of a domain, define what constitutes a domain, posit how new domains are created over time, and describe the features of what is and is not a domain. These definitions and features lead to our proposal that the "Information Sphere" should the preferred international term, and it is this "InfoSphere" that qualifies as a new domain, with features both similar to and different from the four existing physical domains.

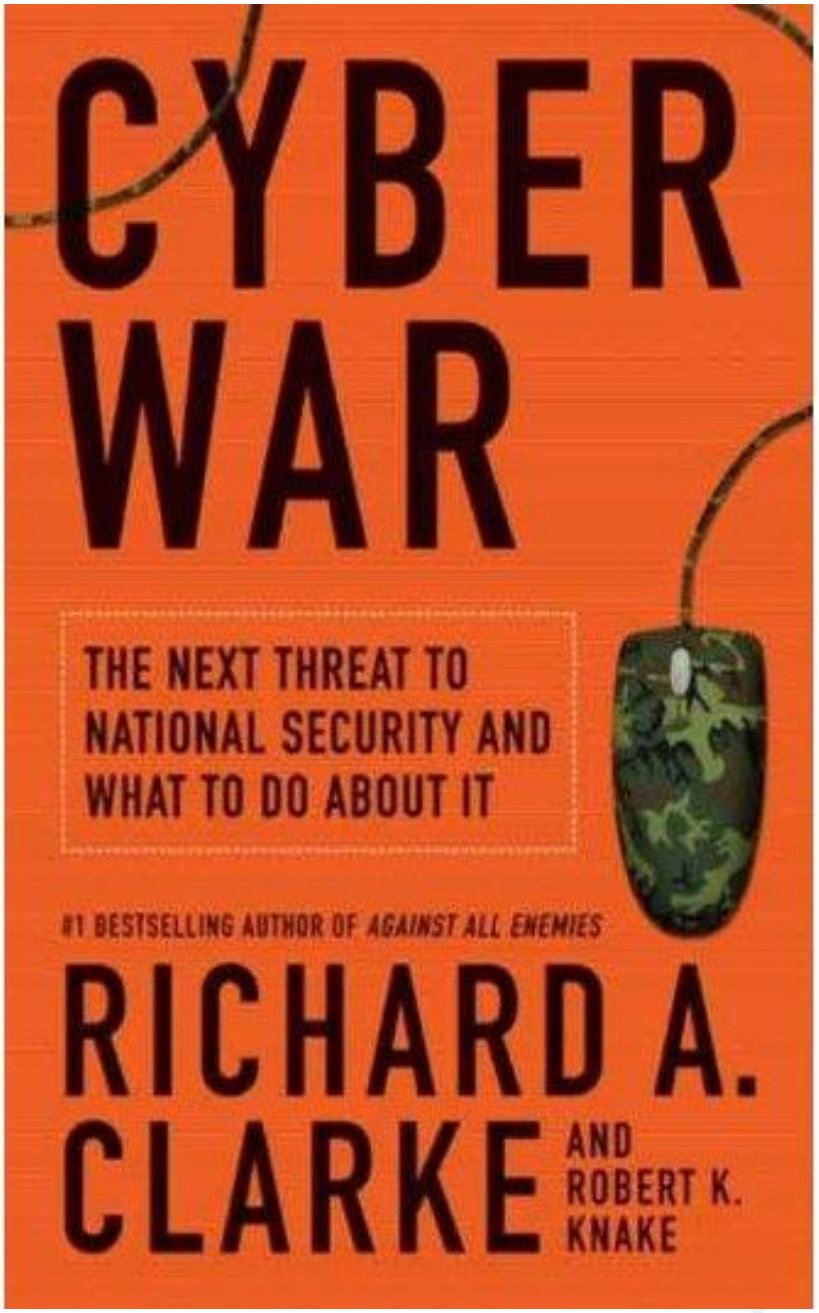
Keywords. domain, information, cyber, cyberspace

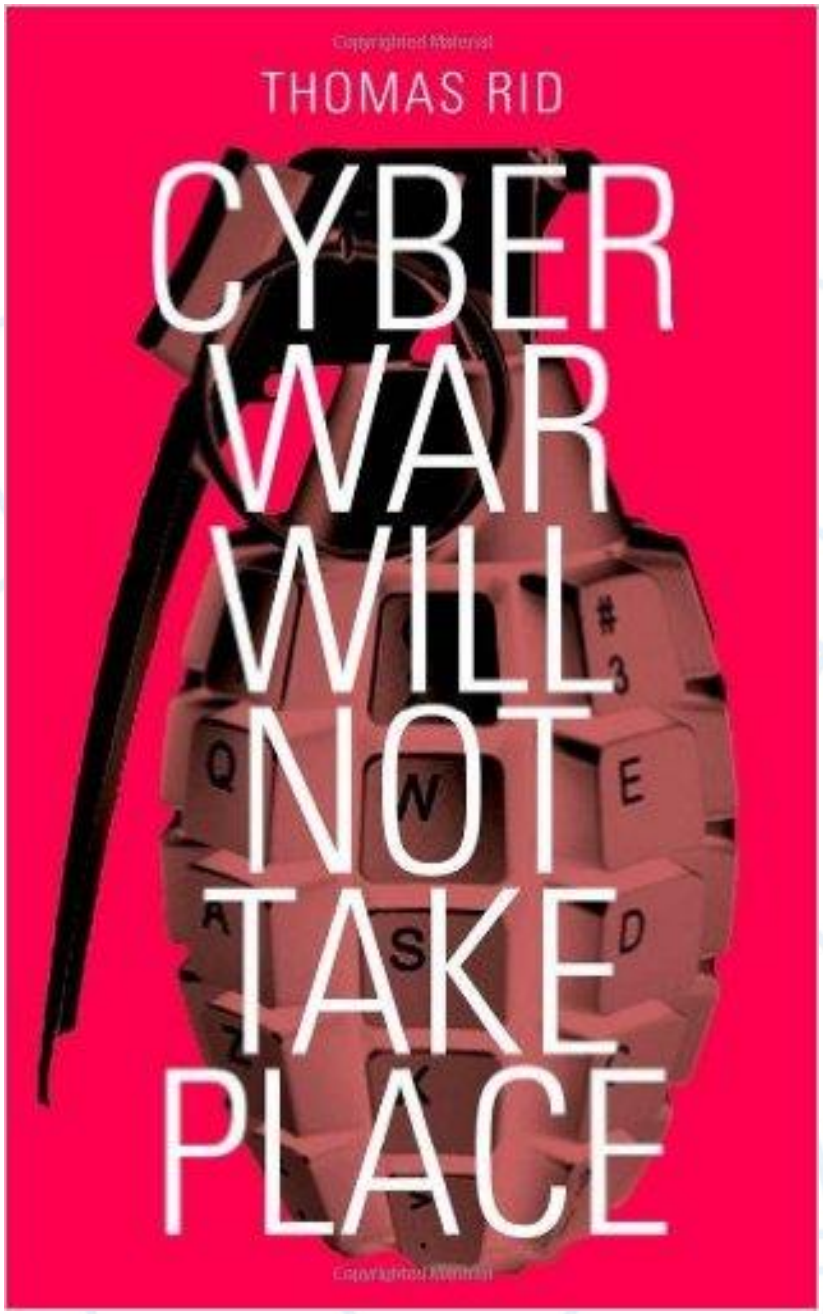
Introduction

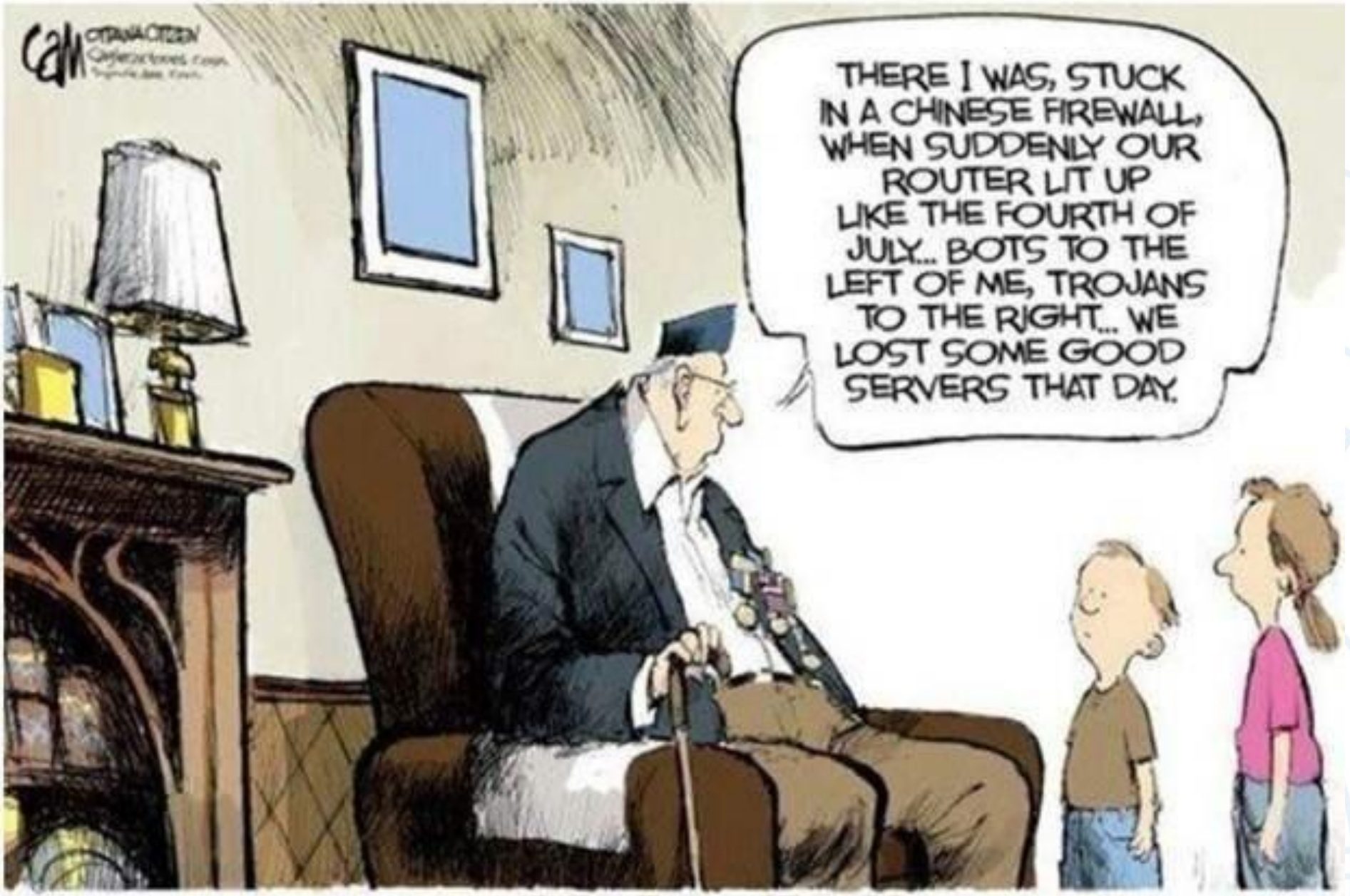
Since classical times, two domains of operation dominated military and civilian operations: land and sea. The advent of powered flight in 1904 initiated the opportunity for a third domain. Shortly thereafter, actions by opposing elements in this airspace began during World War I. The Army and Navy each developed its own air capabilities, and at the end of World War II, the Army Air Corps became the US Air Force—about 50 years after the first powered flight. In a similar manner, the dawn of the "space age" in 1955 encouraged each of the U.S. military services to invest in their own efforts in the space domain. By the mid to late 1980's, with the advent of then US President Ronald Reagan's Strategic Defense Initiative (SDI), the US DoD acknowledged outer space as a fourth war fighting domain.

Based on the preceding observations, the historical trends for recognizing new domains tend to follow this sequence:

- First, the *capability* to begin to operate in that domain is developed, such as the first powered flight or the first space flight.
- Second, the capabilities to operate in that domain become relatively *commonplace*, such as air travel or Shuttle launches.


CYBER WAR
THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT
#1 BESTSELLING AUTHOR OF AGAINST ALL ENEMIES
RICHARD A. CLARKE AND ROBERT K. KNAKE


THOMAS RID
CYBER WAR WILL NOT TAKE PLACE



FUTURE WAR STORIES

CCDCOE