Cyber war unlikely: study

January 17 2011

Sailors on the watch-floor of the US Navy Cyber Defence Operations Command monitor. Credit: US Navy

(PhysOrg.com) -- Heavy lobbying, lurid language and poor analysis are inhibiting government planning for cyber protection, according to a new report on Systemic Cyber Security published by the *Organization for Economic Cooperation and Development* (OECD) on 17 January 2011.

The study, by Dr. Ian Brown of the Oxford Internet Institute (OII), University of Oxford, and Professor Peter Sommer of the London School of Economics also concludes that it is highly unlikely there will ever be a pure 'cyber war' fought solely in cyberspace with equivalent effects to recent wars in Afghanistan, the Balkans or the Middle East.

The report, part of a wider OECD project on Future Global Shocks, is aimed at governments, global businesses and policy makers. It looks at the nature of global catastrophes and then asks which possible cyber-events might create similar effects. In addition to the actions of governments and terrorists the study also considers criminals and accidents. There is a review of current government action, an examination of how governments interact with the private sector and a consideration of the prospects for international cooperation and treaties.

The best protections are careful system design, the use of products to detect known viruses and system intrusions, and user education, says the report. It adds that it is also essential to have proper contingency plans for system recovery.

Dr. Brown commented: "We think that a largely military approach to cybersecurity is a mistake. Most targets in the critical national infrastructure of communications, energy, finance, food, government, health, transport, and water are in the private sector. Because it is often difficult to be certain who is attacking you from cyberspace, defence by deterrence does not work."

"That said, cyberweaponry in all its forms will play a key role alongside more conventional and psychological attacks by nation states in future warfare."

"We don’t help ourselves using “cyberwar” to describe espionage or hacktivist blockading or defacing of websites, as recently seen in reaction to WikiLeaks," said Professor Sommer, visiting professor at LSE. "Nor is it helpful to group trivially avoidable incidents like routine viruses and frauds with determined attempts to disrupt critical national infrastructure."

The study says that many ‘cyber’ risks are real but that it is important to test each one to understand all the elements that are required before a potential threat causes real damage. How much research is required on the target, in writing computer code that won’t be detected, and how long will the event last before the attacked system is able to recover? It says this type of careful analysis helps us understand what we should really worry about and points the way to remedies.

The study is part of a broader OECD review of Future Global Shocks which covers pandemics and further collapse of the world financial system.

The UK Government has announced as part of its Strategic Defence and Security Review that £650m is available to address ‘cyber’ attacks, seen as a Tier One threat.

Provided by Oxford University

Citation: Cyber war unlikely: study (2011, January 17) retrieved 8 May 2024 from https://phys.org/news/2011-01-cyber-war.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.