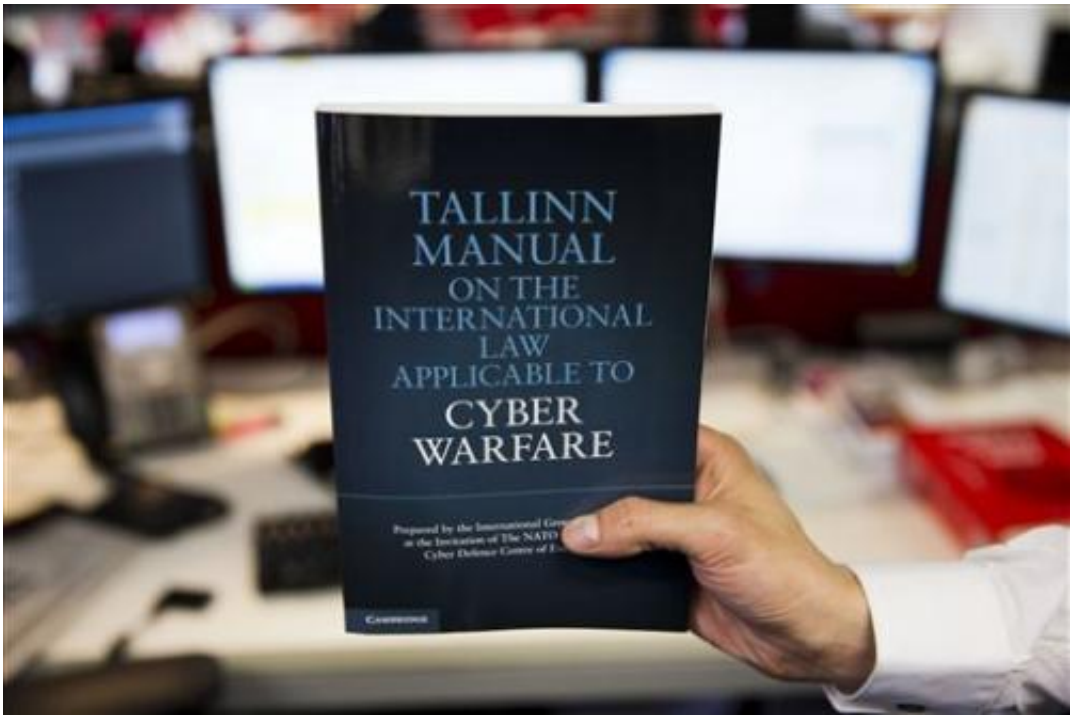
Cyberwar manual lays down rules for online attacks (Update 3)

March 19 2013, by Raphael Satter



A copy of the Tallinn Manual, a rulebook on cyberwarfare, is held up in a posed photograph in London, Tuesday, March 19, 2013. Even cyberwar has rules, and one group of experts is publishing a manual to prove it. The handbook due to be published later this week applies the venerable practice of international law to the world of electronic warfare in an effort to show how hospitals, civilians, and neutral nations can be protected in an information age fight. (AP Photo/Matt Dunham)

Even cyberwar has rules, and one group of experts is putting out a

manual to prove it. Their handbook, due to be published later this week, applies the practice of international law to the world of electronic warfare in an effort to show how hospitals, civilians and neutral nations can be protected in an information-age fight.

"Everyone was seeing the Internet as the 'Wild, Wild West,'" U.S. Naval War College Professor Michael Schmitt, the manual's editor, said in an interview before its official release. "What they had forgotten is that international law applies to cyberweapons like it applies to any other weapons."

The Tallinn Manual—named for the Estonian capital where it was compiled—was created at the behest of the NATO Cooperative Cyber Defense Center of Excellence, a NATO think tank. It takes existing rules on battlefield behavior, such as the 1868 St. Petersburg Declaration and the 1949 Geneva Convention, to the Internet, occasionally in unexpected ways.

Marco Roscini, who teaches international law at London's University of Westminster, described the manual as a first-of-its-kind attempt to show that the laws of war—some of which date back to the 19th century—were flexible enough to accommodate the new realities of online conflict.

The 282-page handbook has no official standing, but Roscini predicted that it would be an important reference as military lawyers across the world increasingly grapple with what to do about electronic attacks.

"I'm sure it will be quite influential," he said.

The manual's central premise is that war doesn't stop being war just because it happens online. Hacking a dam's controls to release its reservoir into a river valley can have the same effect as breaching it with

explosives, its authors argue.

Legally speaking, a cyberattack that sparks a fire at a military base is indistinguishable from an attack that uses an incendiary shell.

The humanitarian protections don't disappear online either. Medical computers get the same protection that brick-and-mortar hospitals do. The personal data related to prisoners of war has to be kept safe in the same way that the prisoners themselves are—for example by having the information stored separately from military servers that might be subject to attack.

Cyberwar can lead to cyberwar crimes, the manual warned. Launching an attack from a neutral nation's computer network is forbidden in much the same way that hostile armies aren't allowed to march through a neutral country's territory. Shutting down the Internet in an occupied area in retaliation for a rebel cyberattack could fall afoul of international prohibitions on collective punishment.

The experts behind the manual—two dozen officers, academics, and researchers drawn mainly from NATO states—didn't always agree on how traditional rules applied in a cyberwar.

Self-defense was a thorny issue. International law generally allows nations to strike first if they spot enemy soldiers about to pour across the border, but how could that be applied to a world in which attacks can happen at the click of a mouse?

Other aspects of international law seemed obsolete—or at least in need of an upgrade—in the electronic context.

Soldiers are generally supposed to wear uniforms and carry their arms openly, for example, but what relevance could such a requirement have

when they are hacking into distant targets from air-conditioned office buildings?

The law also forbids attacks on "civilian objects," but the authors were divided as to whether the word "object" could be interpreted to mean "data." So that may leave a legal loophole for a military attack that erases valuable civilian data, such as a nation's voter registration records.

More information: The Tallinn Manual: www.ccdcoe.org/249.html