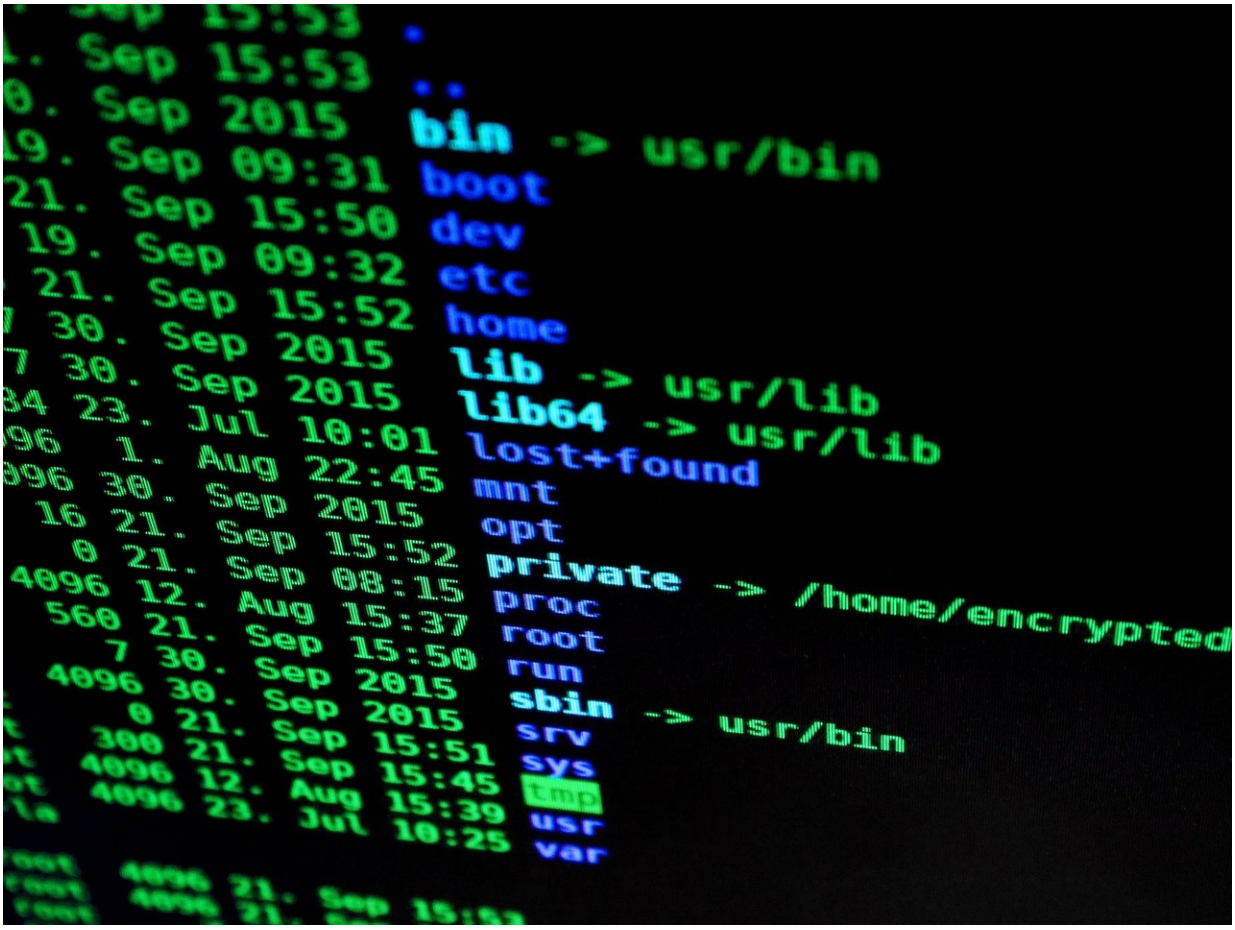
Red Cross chief: cyber attacks increasing on hospitals

August 27 2020, by Edith M. Lederer



Credit: CC0 Public Domain

The president of the International Committee of the Red Cross warned

Wednesday that the frequency of sophisticated cyber attacks against hospitals, electricity and water supplies, and other critical civilian infrastructure is increasing.

Peter Maurer said the ICRC is increasingly concerned about the destructive effects of cyber operations that cut off electricity supplies and water systems in war-affected countries and halted hospital services in the middle of the COVID-19 pandemic as well as "an attempted attack against a petrochemical plant and especially alarmingly, cyber-attacks against nuclear facilities."

"If hospitals cannot provide life-saving treatment in the middle of a health crisis or an armed conflict, whole communities will suffer," he told an informal virtual meeting of the U.N. Security Council.

"If electricity supply is interrupted, there is a real risk that water, health care, and other essential services will be disrupted," the ICRC chief said. "And if even nuclear facilities are not considered off limits, we risk seeing severe and widespread humanitarian consequences."

Over recent years, Maurer said, cyber attacks against critical infrastructure "have caused significant economic harm, disruption in societies, and tensions" among nations although the ICRC can't confirm any cyber operations that have resulted in human casualties.

He said the frequency of cyber attacks against civilian infrastructure "is increasing and evolving faster than anticipated only a few years ago."

While most appear not to be linked to conflict, he said, "we are concerned that cyber capabilities used in future conflicts will cause graver consequences, in particular for civilians."

Several countries have stated publicly in recent years that they used

cyber operations in military actions, Maurer said, and "as an increasing number of states are developing military cyber capabilities, the ICRC expects that their use is likely to also increase in future conflicts."

He welcomed the Security Council's engagement on the issue of harmful cyber operations, alongside ongoing discussions in the U.N. General Assembly.

Russia won General Assembly approval in December for a resolution that will start the process of drafting a new international treaty to combat cyber crime over objections from the European Union, the U.S. and others. They said it would undermine international cooperation to combat cyber crime. Russia has said substantive work on the new convention will begin in 2021.

Maurer said preventive measures are needed.

The ICRC has called on all countries "to reaffirm and clarify the legal framework that protects critical civilian infrastructure against cyber operations," especially particular during conflict including health systems, water and sanitation systems, electricity supply and "installations containing dangerous forces," he said.

But Maurer cautioned that a strong legal framework "is not by itself sufficient to effectively shield civilians and civilian infrastructure from hostile cyber operations."

He said confidence-building measures and a broad range of technical and operational measures are also needed.

"No state can succeed in this alone," Maurer said. "Instead, broad collaboration among states, as well as between states, the private sector, and academia is essential."