By Huw Jones

STRASBOURG, France (Reuters) - Estonia called on the European Union on Wednesday to make cyber attacks a criminal offense to stop Internet users from freezing public and private Web sites for political revenge.

Estonian President Toomas Hendrik Ilves said he believed the Russian government was behind an online attack on Estonia over its decision to move a Red Army monument from a square in the capital Tallinn. Russia has denied any involvement.

The decision triggered two nights of rioting by mainly Russian-speaking protesters, who argued that the Soviet-era memorial was a symbol of sacrifices made during World War Two.

The rioting coincided with repeated requests to Web sites, forcing them to crash or freeze. Network specialists said at the time at least some of the computers used could be traced to the Russian government or government agencies.

"Russian officials boasted about having done it (cyber attacks) afterwards – one in a recent interview a month and a half ago saying we can do much more damage if we wanted to," he told Reuters in an interview.

"We now have a much clearer understanding that we need to have a legislative basis for prosecuting cyber crime because it is a crime," Ilves said.

"That is something we are pushing for within the European Union and within NATO as well, where we can. It's almost by definition a cross-border crime," Ilves added.

"The UK has good legislation and the United States has good legislation. France has better than most and the rest of the EU does not really have this kind of legislation," Ilves said.

The European Commission has sole right to initiate EU law and its Information Society and Media Commissioner Viviane Reding agreed action was needed.

"What happened in Estonia should be a wake-up call for Europe. Cyber attacks on one member state concern the whole of Europe. They must therefore receive a firm European response," Reding told Reuters from Budapest.

Reding said that last November she proposed setting up a new European telecoms market authority.

NATO also has opened a cyber defense "centre of excellence" in Estonia to study solutions to combating online attacks.

Ilves said he believed the attacks had been paid for.

"Looking at the graph of the attacks that came, when they stopped all at once at (midnight) I asked the computer emergency response team why it stopped so suddenly. They said the money ran out," Ilves said.

Mock cyber attacks on Estonia's new online voting system have given the country a better idea of how to handle a real attack when it came, Ilves said.

"Other (EU) member states helped in fending off the attacks by siphoning off some of the attacks," Ilves said.