

Richard Clarke On The Growing 'Cyberwar' Threat



Enlarge

iStockphoto.com

Clarke says he would like to see a separate government Internet network that would be constantly monitored for signs of attack.

Cyber War: The Next Threat to National Security and What to Do About It

By Richard Clarke and Robert K. Knake
Hardcover, 304 pages
Ecco

List price: \$25.99

[Read An Excerpt](#)

though the government has set up security measures to protect military and intelligence networks, he worries that not enough is being done to protect the private sector -- which includes the electrical grid, the banking system and our health care records.

[Read A Timeline Of Major Cybersecurity Incidents Since 2007](#)

doesn't today -- but everybody else will have to do their own defense. That is a formula that will not work in the face of sophisticated threats."

Related NPR Stories

Countries Try To Tame The Wild Territory Of The Net
April 8, 2010

Cyber Insecurity: U.S. Struggles To Confront Threat
April 6, 2010

Assessing The Threat Of Cyberterrorism
Feb. 10, 2010

Richard Clarke: 'Government Failed You' on Security
May 28, 2008



Mark Wilson/Getty Images

Richard Clarke resigned from the Bush administration in 2003. He served as the national coordinator for counterterrorism in the Clinton and George W. Bush administrations — and was the special adviser to President Bush on

April 19, 2010

text size **A A A**

Richard Clarke served as a counterterrorism adviser to Presidents Bill Clinton and George W. Bush. He spent much of 2001 warning members of the Bush administration about the possibility of an impending al-Qaida attack.

Clarke has now turned his attention to another potential security catastrophe: computer-based terrorism attacks. In his new book, *Cyberwar: The Next Threat to National Security and What to Do About It*, he and co-author Robert Knake sketch out a scenario in which hackers could hypothetically cripple the United States from behind a computer screen.

"A cyberattack could disable trains all over the country," he tells *Fresh Air* host Terry Gross. "It could blow up pipelines. It could cause blackouts and damage electrical

power grids so that the blackouts would go on for a long time. It could wipe out and confuse financial records, so that we would not know who owned what, and the financial system would be badly damaged. It could do things like disrupt traffic in urban areas by knocking out control computers. It could, in nefarious ways, do things like wipe out medical records."

Clarke says that cyberattacks can come from another country -- or from a lone individual. Malicious code may infect a computer via a security flaw in a Web browser, or it could be distributed through secret back doors built into computer hardware. And

"The Pentagon is all over this," he says. "The Pentagon has created a four-star general command called Cyber Command, which is a military organization with thousands of people in it to go to war using these [cyber]weapons. And also, Cyber Command's job is to defend the Pentagon. Now, who's defending us? Who's defending those pipelines and the railroads and the banks? The Obama administration's answer is pretty much, 'You're on your own,' that Cyber Command will defend our military, Homeland Security will someday have the capability to defend the rest of the civilian government -- it

Clarke says that one common attack is for hackers to take over a series of home computers through backdoor security exploits. For example, malicious software can be downloaded onto a hard drive after you accidentally visit a compromised website. Your computer can then be used in conjunction with other compromised computers to engage in a large-scale attack. The average computer user may not realize when their computer has been drafted into a cyberattack.

"Maybe your computer will be running a little slowly that day," he says. "Maybe your bandwidth won't look like it's normal. But while you're doing your e-mails, your computer could be sending out denial of service attacks as part of a million other computers all trying to knock off a bank."

There are ways to make your computer less vulnerable to one of these attacks. Clarke recommends never using your work computer at home, where it may be unintentionally compromised by another member of your family. And, he says, make sure your online banks have more than just a password for security protection.

"Good hackers can get through any password," he says. "If you're going to buy things online, have a credit card for that purpose with a low credit limit. Don't do banking or stockbrokering online and have a lot of money at risk -- unless your stockbroker gives you more than just a password -- a two-step process for getting in. It won't just be a name and password."

Clarke now heads a security consulting firm in Virginia and is a contributor to ABC News. He also teaches at Harvard's Kennedy School of Government. His 2004 memoir is entitled *Against All Enemies: Inside America's War on Terror*. He is also the author of *Your Government Failed You: Breaking the Cycle of National Security Disasters and The Scorpion's Gate*.

