

Cyber weaknesses should deter US from waging war

November 8 2011, LOLITA C. BALDOR , Associated Press



In this Feb. 19, 2010 photo, Richard A. Clarke, a former advisor to the president for security, attends a news conference of the film "S.O.S. - State of Security" at the International Film Festival Berlinale in Berlin. Clarke says America's computer systems are so vulnerable to attack that it should deter U.S. leaders from going to war with other nations. (AP Photo/Markus Schreiber)

(AP) -- America's critical computer networks are so vulnerable to attack that it should deter U.S. leaders from going to war with other nations, a former top U.S. cybersecurity official said Monday.

Richard Clarke, a top adviser to three presidents, joined a number of U.S. military and civilian experts in offering a dire assessment of America's [cybersecurity](#) at a conference, saying the country simply can't protect its critical networks.

Clarke said if he was advising the president he would warn against attacking other countries because so many of them - including [China](#), [North Korea](#), Iran and Russia - could retaliate by launching devastating cyberattacks that could destroy [power grids](#), banking networks or transportation systems.

The U.S. military, he said, is entirely dependent on computer systems and could end up in a future conflict in which troops trot out onto a battlefield "and nothing works."

Clarke said a good national security adviser would tell the president that the U.S. might be able to blow up a [nuclear plant](#) somewhere, or a terrorist training center somewhere, but a number of countries could strike back with a [cyberattack](#) and "the entire us economic system could be crashed in retaliation ... because we can't defend it today."

"I really don't know to what extent the weapon systems that have been developed over the last 10 years have been penetrated, to what extent the chips are compromised, to what extent the code is compromised," Clarke said. "I can't assure you that as you go to war with a cybersecurity-conscious, cybersecurity-capable enemy that any of our stuff is going to work."

Clarke, along with Gen. Keith Alexander, who heads both the [National Security Agency](#) and U.S. Cyber Command, told the conference crowd that the U.S. needs to do a better job at eliminating network vulnerabilities and more aggressively seek out malware or viruses in American corporate, military and [government systems](#).

But Clarke was more strident about pushing for broader government regulations to enforce such improvements, despite political reluctance. The problems, he said, will not be fixed unless the government gets more involved.

He added that the U.S. also needs to make it clear to countries such as China that efforts to use computer-based attacks to steal high-tech American data will be punished.

In a forceful and detailed public report last week, U.S. intelligence officials accused China and Russia of systematically stealing sensitive U.S. economic information and technologies for their own national economic gain.

The report called on the U.S. to confront China and Russia in a broad diplomatic push to combat cyberattacks that are on the rise and which represent a "persistent threat to U.S. economic security."

On Monday, Clarke said that until there are real consequences for the massive espionage, countries like China will still keep stealing.

©2011 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Citation: Cyber weaknesses should deter US from waging war (2011, November 8) retrieved 25 April 2024 from <https://phys.org/news/2011-11-cyber-weaknesses-deter-waging-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.