Internet vandals threaten access and expression on the World Wide Web

The Editorial Board
11 February 2000

The source of the coordinated attacks that crippled major Internet web sites earlier this week and the motivations of those responsible remain unclear. But whoever carried out these actions, and whatever their subjective purpose, the objective content of the assault on the Internet was a reactionary attack on democratic rights.

The attempt to exploit the relatively open character of the Internet to cripple targeted sites is an act of sabotage that can have no progressive content. Moreover, it can only strengthen those commercial and government forces that want to clamp down on the World Wide Web and restrict the free flow of information and debate along this powerful international medium.

On three successive days, leading web sites were hit by a form of hacker attack known as “denial of service” (DOS). While the technology involved in such an assault is not sophisticated, the scale of the attacks indicate considerable advanced planning and, in all probability, the coordinated efforts of at least several hackers.

In a DOS attack, a hacker programs a computer, or group of computers, to repeatedly call up a web site, perhaps thousands of times a second. This overloads the site and either shuts it down completely or blocks access to legitimate users. It is believed those responsible for this week's attacks first planted an illicit program in dozens, if not hundreds, of unsuspecting Internet-linked computers. They then triggered these computers to simultaneously flood the targeted web sites with thousands of messages and requests for information.

On Monday the Internet clearinghouse Yahoo, whose daily traffic (42 million unique visitors) is second only to America Online, was shut down for three hours. On Tuesday the online bookseller Amazon suffered a major slowdown, Time Warner's CNN news site was shut for two hours, and the e-commerce retailers Ebay and Buy.com were either jammed or completely closed for a good part of the day. On Wednesday the technology news site ZDNet was forced off-line for two hours and the on-line brokerage E-Trade suffered sporadic outages for several hours.

Major Internet providers such as MCI WorldCom's UUNet division and Microsoft's MSN network also reported slowdowns and disruptions as a result of the attacks on the targeted sites. Keynote Systems, a company that measures the performance of web sites, reported Wednesday that during the assaults it took eight seconds to call up a typical web site's home page, nearly twice the time required over the previous two weeks.

In Washington Attorney General Janet Reno announced that the FBI had opened a criminal investigation into the cyber attacks. Reno said the Justice Department was “not aware of the motives behind these attacks.” However some observers suggested that the timing might not have been random. They pointed out that many of the country's top Internet security experts were attending the North American Network Operators' Group conference in San Jose, California when the attacks began. The assault on Yahoo began only minutes after an Internet security expert from AT&T Labs ended a speech on DOS attacks and how to secure sites against them.

These acts of cyber vandalism play directly into the hands of government agencies that have been pressing for increased police powers over the Internet. The FBI investigation will doubtless be used to test the ability of the state to monitor Internet traffic and pinpoint the origin of messages. The FBI has already begun

examining the records of the target companies and their partners on the Web. It is collecting logs from Internet service providers that can show where transmissions originated.

FBI Director Louis Freeh has been pushing for Congress to grant the bureau greater power to make the nation's telephone and computer networks more accessible to wire-taps and other forms of surveillance. Last July, the Clinton administration circulated a plan for an extensive software system to monitor government computers and possibly those of private industry. The network, known as the Federal Intrusion Detection Network, or Fidnet, alarmed civil libertarians who said it could be used to curtail privacy on the Internet.

It is too soon to say whether those responsible for this week's attacks come from the milieu of anti-cyber activists who consider modern technology itself to be an evil force. But even if that proves not to be the case, the latest assault on the Internet underscores the deeply reactionary essence of this particular form of middle-class politics. Far from expressing a democratic spirit, the modern-day Luddites evince a morbid pessimism and contempt for the capacity of working people to build a popular movement for progressive and revolutionary change.

Nor do those who seek to undermine the Internet actually oppose its increasing subordination to big business, and the restriction of political and intellectual expression which is an inevitable byproduct of the commercialization of the medium. On the contrary, they aid the corporate/government drive to eviscerate the Internet's democratic potential.

Events such as this week's cyber attacks complement the anti-democratic tendencies inherent in the growing monopolization of the Internet and the telecommunications industry as a whole, embodied in the recently announced merger of America Online and Time Warner.