Trevor Butterworth

Stuxnet was a valuable warning shot.

Congress may be throwing a fit over intelligence leaks that implicate the United States in an elaborate cyberattack against Iran's nuclear program, but to some of the world's leading cybersecurity experts, the revelations, far from doing harm, may actually do the world a favor.

"This is nothing if not a good opportunity to accept reality," says Rodney Joffe, senior vice president and senior technologist at Neustar. Stuxnet—and its newly identified kissing cousin in cybermischief, Flame—should not be seen as fiendish pieces of technology that the military let loose and then lost through careless coding and opportunistic leaking, but something that hackers were doing long before the military muscled in. It is simply "naive," he says, to think that only the military is capable of such sophistication. China's industrial base practically depends on hacking for innovation, he explains. And yet the attitude among many CEOs is that they're safe from cyberattack.

Richard Bejtlich, chief security officer for the information-security company Mandiant, concurs, noting that many politicians are woefully unaware of the new status quo of national insecurity; and while he, as a former Air Force intelligence officer, is appalled by some of the recent leaks about military operations, he says the Stuxnet incident provides a valuable teaching moment. "We're hurtling down the path of being ever more dependent on our networks," he says. And that infrastructure is alarmingly fragile, particularly the electrical grid. "The chaos that would ensue if it were attacked would be ridiculous."

Toomas Hendrik Ilves, Estonia's president, emerged as one of the world's leading political thinkers on cybersecurity after his country came under sustained cyberattack in 2007. Ilves's message is almost counterintuitive from a national security perspective. "A free, open, and transparent Internet is central to global cybersecurity," he tells Newsweek. "We can best defend ourselves against cyberattacks if we share information openly and collaborate to defeat threats." This is, after all, how Stuxnet and Flame were discovered. "It was open and public dissemination of information about the malware that raised the alarm, disseminated patches and fixes, and mitigated their threat to our societies," he explains.

Joffe says the next step is to build the 21st century's equivalent of a radar network to monitor cyberthreats and share information. After that comes the trickier job of inventing new tools to protect people and, ultimately, devising more robust protocols to run the Internet. In this, the U.S. has one diminishing advantage: "The terrorist guys are still old school, says Bejtlich, "and they like to see things blow up."

Original article on the Newsweek webpage .