Battling the Cyber Warmongers

Cyberattacks are inevitable but the threat has been exaggerated by those with a vested interest

By EVGENY MOROZOV

A recent simulation of a devastating cyberattack on America was crying for a Bruce Willis lead: A series of mysterious attacks—probably sanctioned by China but traced to servers in the Russian city of Irkutsk—crippled much of the national infrastructure, including air traffic, financial markets and even basic email. If this was not bad enough, an unrelated electricity outage took down whatever remained of the already unplugged East Coast.

The simulation—funded by a number of major players in network security, organized by the Bipartisan Policy Center, a Washington-based think tank, and broadcast on CNN on a Saturday night—had an unexpected twist. The American government appeared incompetent, indecisive and confused (past government officials, including former Secretary of Homeland Security Michael Chertoff and former Deputy Secretary of State John Negroponte, were recruited to play this glamorous role on TV). “The U.S. is unprepared for cyberwar,” the simulation’s organizers grimly concluded.

The past few months have been packed with cyber-jingoism from former and current national security officials. Richard Clarke, a former cybersecurity adviser to two administrations, says in his new book that “cyberwar has already begun.” Testifying in Congress in February, Mike McConnell, former head of the National Security Agency, argued that if we went to war today in a cyberwar, we would lose.” Speaking in late April, Director of Central Intelligence Leon Panetta said that “the next Pearl Harbor is likely to be a cyberattacking going after our grid.”

The murky nature of recent attacks on Google—in which someone tricked a Google employee into opening a malicious link that eventually allowed intruders to access parts of Google’s password-managing software, potentially compromising the security of several Chinese human rights activists—has only added to public fears. If the world’s most innovative technology company cannot protect its computers from such digital aggression, what can we expect from the bureaucratic chimera that is the Department of Homeland Security?

http://online.wsj.com/article/SB100014240527487043704575228653351323986.html
Google should be applauded for going on the record about the cyber-attacks; most companies prefer to keep quiet about such incidents. But do hundreds—or even thousands—of such incidents that target both the private and the public sector add up to the imminent threat of a “cyberwar” that is worthy of such hype? The evidence so far looks too shaky.

Ironically, the more we spend on securing the Internet, the less secure we appear to feel. A 2009 report by Input, a marketing intelligence firm, projected that government spending on cybersecurity would grow at a compound rate of 8.1% in the next five years. A March report from consulting firm Market Research Media estimates that the government’s total spending on cybersecurity between now and 2015 is set to hit $55 billion, with strong growth predicted in areas such as Internet-traffic surveillance and monitoring.

Given the previous history of excessively tight connections between our government and many of its contractors, it’s quite possible that the over-dramatized rhetoric of those cheerleading the cyberwar has helped to add at least a few billion dollars to this price tag. Mr. McConnell’s current employer, Booz Allen Hamilton, has just landed $34 million in cyber security contracts with the Air Force. In addition to writing books on the subject, Richard Clarke is a partner in a security firm, Good Harbor Consulting.

“The point we have made about cyberwar is that the U.S. has created a large and expensive cyberwar command, as have other nations. Thus, the government thinks cyberwar is possible no matter what the naysayers think,” says Mr. Clarke in an email. Mr. Clarke says 90% of his firm’s revenue in 2009 and 2010 to date comes from consulting unrelated to cybersecurity, and none of the proposals from his book would financially benefit Good Harbor. In a statement, Booz Allen Hamilton says of Mr. McConnell: “As director of national intelligence he delivered the same messages of concern about the vulnerability of our cyber-infrastructure to President George W. Bush and presidential candidate Barack Obama…As a longstanding intelligence professional, McConnell has an awareness across the full spectrum of classification, and sees it as his duty in public service to foster the right kind of discussion so the nation’s leadership can debate and mitigate the risks.”

Cyberspace’s Big Bullies

From ‘Dark Dante’ to the originator of the Internet worm, a selection of notorious hackers.

Kevin Poulsen

Both Messrs. McConnell and Clarke—as well as countless others who have made a successful transition from trying to fix the government’s cyber security problems from within to offering their services to do the same from without—are highly respected professionals and their opinions should not be taken lightly, if only because they have seen more classified reports. Their stature, however, does not relieve them of the responsibility to provide some hard evidence to support their claims. We do not want to sleepwalk into a cyber-Katrina, but neither do we want to hold our policy-making hostage to the rhetorical ploys of better-informed government contractors.

Steven Walt, a professor of international politics at Harvard, believes that the nascent debate about cyberwar presents "a classical
opportunity for threat inflation." Mr Walt points to the resemblance between our current deliberations about online security and the debate about nuclear arms during the Cold War. Back then, those working in weapons labs and the military tended to hold more alarmist views than many academic experts, arguably because the livelihoods of university professors did not depend on having to hype up the need for arms racing.

Markus Ranum, a veteran of the network security industry and a noted critic of the cyber war hype, points to another similarity with the Cold War. Today's hype, he says, leads us to believe that "we need to develop an offensive capability in order to defend against an attack that isn't coming—it's the old 'bomber gap' all over again: a flimsy excuse to militarize."

How dire is the threat? Ask two experts and you will get different opinions. Just last month, Lt. Gen. Keith Alexander, director of the NSA, told the Senate's Armed Services Committee that U.S. military networks were seeing "hundreds of thousands of probes a day." However, speaking at a March conference in San Francisco, Howard Schmidt, Obama's recently appointed cybersecurity czar, said that "there is no cyberwar," adding that it is "a terrible metaphor" and a "terrible concept."

The truth is, not surprisingly, somewhere in between. There is no doubt that the Internet brims with spamming, scamming and identity fraud. Having someone wipe out your hard drive or bank account has never been easier, and the tools for committing electronic mischief on your enemies are cheap and widely accessible.

This is the inevitable cost of democratizing access to multi-purpose technologies. Just as any blogger can now act like an Ed Murrow, so can any armchair-bound cyberwarrior act like the über-hacker Kevin Mitnick, who was once America's most-wanted computer criminal and now runs a security consulting firm. But just as it is wrong to conclude that the amateurization of media will bring on a renaissance of high-quality journalism, so it is wrong to conclude that the amateurization of cyberattacks will usher in a brave new world of destructive cyberwarfare.

In his Senate testimony—part of his confirmation process to head the Pentagon's new Cyber Command—Gen. Alexander of the NSA explained those "hundreds of thousands of probes" could allow attackers to "scan the network to see what kind of operating system you have to facilitate...an attack." This may have scared our mostly technophobic senators but it's so vague that even some of the most basic attacks available via the Internet—including those organized by "script kiddies," or amateurs who use scripts and programs developed by professional hackers—fall under this category. Facing so many probes is often the reality of being connected to the Internet. The number of attacks is not a very meaningful indicator of the problem, especially in an era when virtually anyone can launch them.

From a strictly military perspective, "cyberwar"—with a small "c"—may very well exist, playing
second fiddle to ongoing military conflict, the one with tanks, shellfire and all. The Internet—much like the possibility of air combat a century ago—has opened new possibilities for military operations: block the dictator’s bank account or shut down his propaganda-infested broadcast media. Such options were already on the table—even though they appear to have been used sparingly—during a number of recent wars. Back in 1999, Gen. Wesley Clark, then the outgoing supreme allied commander in Europe, instilled American policy makers with high hopes when he said in Senate testimony that NATO could have “methods to isolate Milosevic and his political parties electronically,” thus preventing “the use of the military instrument.”

Why have such tactics—known in military parlance as “computer network attacks”—not been used more widely? As revolutionary as it is, the Internet does not make centuries-old laws of war obsolete or irrelevant. Military conventions, for example, require that attacks distinguish between civilian and military targets. In decentralized and interconnected cyberspace, this requirement is not so easy to satisfy: A cyberattack on a cellphone tower used by the adversary may affect civilian targets along with military ones. When in 2008 the U.S. military decided to dismantle a Saudi Internet forum—initially set up by the CIA to glean intelligence but increasingly used by the jihadists to plan attacks in Iraq—it inadvertently caused disruption to more than 300 servers in Saudi Arabia, Germany and Texas. A weapon of surgical precision the Internet certainly isn’t, and damage to civilians is hard to avoid. Military commanders do not want to be tried for war crimes, even if those crimes are committed online.

As Gen. Clark pointed out in 1999, cyberwarfare may one day give us a more humane way to fight wars (why, for example, bomb a train depot if you can just temporarily disable its computer networks?), so we shouldn’t reject it out of hand. The main reason why this concept conjures strong negative connotations is because it is often lumped with all the other evil activities that take place online—cybercrime, cyberterrorism, cyber-espionage. Such lumping, however, obscures important differences. Cybercriminals are usually driven by profit, while cyberterrorists are driven by ideology. Cyber-spies want the networks to stay functional so that they can gather intelligence, while cyberwarriors—the pure type, those working on military operations—want to destroy them.

All of these distinct threats require quite distinct policy responses that can balance the risks with the levels of devastation. We probably want very strong protection against cyberterror, moderate protection against cybercrime, and little to no protection against juvenile cyber-hooliganism.

Perfect security—in cyberspace or in the real world—has huge political and social costs, and most democratic societies would find it undesirable. There may be no petty crime in North Korea, but achieving such “security” requires accepting all other demands of living in an Orwellian police state. Just like we don’t put up armed guards to protect every city wall from graffiti, we should not overreact in cyberspace.

Recasting basic government problems in terms of a global cyber struggle won’t make us any more secure. The real question is, “Why are government computers so vulnerable to very basic and unsophisticated threats?” This is not a question of national security; it is a question of basic government incompetence. Cyberwar is the new “dog ate my homework”: It’s far easier to blame everything on mysterious Chinese hackers than to embark on uncomfortable institutional soul-searching.

Thus, when a series of fairly unsophisticated attacks crashed the websites of 27 government agencies—including those of the Treasury Department, Secret Service and Transportation Department—during last year’s July Fourth weekend, it was panic time. North Korea was immediately singled out as their likely source (websites of the South Korean government were also affected). But whoever was behind the attacks, it was not their sophistication or strength that crashed the government’s websites. Network security firm Arbor Networks described the attacks as “pretty modest-sized.” What crashed the websites was the incompetence of the people who ran them. If “pretty modest-sized” attacks can cripple them, someone is not doing their job.

What we do not want to do is turn “weapons of mass disruption”—as Barack Obama dubbed cyberattacks in 2009—into weapons of mass distraction, diverting national attention from more burning problems while promoting extremely costly solutions.
For example, a re-engineering of the Internet to make it easier to trace the location of cyberattackers, as some have called for, would surely be expensive, impractical and extremely harmful to privacy. If today's attacks are mostly anonymous, tomorrow they would be performed using hijacked and fully authenticated computers of old ladies.

What is worse, any major re-engineering of the Internet could derail other ambitious initiatives of the U.S. government, especially its efforts to promote Internet freedom. Urging China and Iran to keep their hands off the Internet would work only if Washington sticks to its own advice; otherwise, we are trading in hype.

In reality, we don't need to develop a new set of fancy all-powerful weaponry to secure cyberspace. In most cases the threats are the same as they were 20 years ago; we still need to patch security flaws, update anti-virus databases and ban suspicious users from our sites. It's human nature, not the Internet, that we need to conquer and re-engineer to feel more secure. But it's through rational deliberation, not fear-mongering, that we can devise policies that will accomplish this.

—Evgeny Morozov is a fellow at Georgetown University and a contributing editor to Foreign Policy. His book about the Internet and democracy will be published this fall.