

Computer Wars

By David Beagan

It is now time to take a fresh look as the true basis of America's status as the world's only superpower. When I was a youngster, I imagine it was the early 1970s, I remember hearing that in the future, wars would be fought by computer. Even though I didn't understand how the two sides might conduct the computer war, it seemed a bit absurd to me. I thought that whichever side lost the computer war, could still just attack with conventional warfare anyway. Why would both side agree to abide by the outcome of the virtual war?

Looking back from today's perspective, I think my reasoning was sound. But what I couldn't have anticipated back then was that the computer would become inextricably linked to all aspects of the infrastructure that we depend upon for daily life. The electrical grid, including nuclear power plants, and innumerable agencies and offices both governmental and private, are built upon a nervous system of interconnected computer networks. The spinal cord of that network is of course the internet. If this computer network suddenly stopped working, the world, at least the modernized western world, would be reduced to third world conditions.

In the early 1980s, a computer game know as Core Wars emerged in academic computer science circles. The object of this game was for computer programs to compete for control of a computer. In the 1990s as the internet emerged as a ubiquitous tool for all computer users, the pranksters and bad guys started playing a game of core wars for real. While computer viruses and other bad programs existed before this, infecting their targets through floppy disks and computer bulletin boards, the internet raised the stakes by an order of magnitude.

Every day, every hour, every second, hackers are probing each our individual computers, but more importantly, probing the computers of businesses, governmental agencies, and the U.S. defense department. You could say that the war has already started. The nature and extent of the defense departments internetwork and its connectedness to the internet would only be a matter of speculation. We have to believe that critical defense department systems have a very controlled and limited access from the outside internet at large. The computer network servers and the connections that comprise this defense department network must be physically isolated from all other networks. But it wouldn't be out of the realm of possibility that some wireless crossover connection could come into existence if some key employee of the government were to be compromised by groups that wish to harm America. Once there is this physical network

breach, one which may go undetected, then the capability for a harmful entity to wreak havoc with America's defense becomes merely a matter of computation and resourcefulness.

We would like to believe that our governmental institutions, that exist for the purposes of protecting us, have the best of technology and the best people implementing and executing that technology. But the sobering fact is, as the attempted Christmas day bombing of flight 253 has shown, that our people and computer systems failed us. The seemingly simple act of discovery, of connecting the informational dots spread across disparate information databases, somehow did not happen. It was only the attempted bombers inexperience and the passengers quick action that averted disaster. If the governmental agencies had stopped the plot, perhaps revoked the attempted bombers visa, we the public would probably never had known about this plot. Other similar plots may have been stopped too. But whatever was different about this one somehow allowed it to get through. Therein lies the problem. There can be a thousand successes in apprehending all manner of potential attacks. But if just one slips through, then they get us. And of course an additional challenge is that there are people who are willing to sacrifice their lives to inflict damage. Thomas Jefferson could never know how true his words would become, "The price of freedom is eternal vigilance."

All failings aside, this shows us that expert application and execution of computer technologies is at the heart of America protecting its freedom. We are not yet in the full computer war era. But now we can see the path to such an era. The minor skirmishes have broken out all over. We can imagine a dark world where chaos rules and the hackers and foreign entities have virtually free reign to disrupt the computer ecosystem. We can also imagine a world where the good guys are able to squelch the hackers and establish a truly safe computing infrastructure. The more realistic outcome is that there is a constant "arms race" where it is always a struggle to stay one step ahead of the evil ones. America's continued preeminence as the world's superpower is fully dependent on its ability to patrol the world's computing infrastructure.

Where man might stop, the computer goes on, for computers know no moral code.

– Boris Raushenbakh
