2006, a senior official in the Syrian government had a serious lapse in judgment. On a visit to London, he left his laptop computer in his hotel room and when he was out, Israeli Mossad agents snuck in and installed a Trojan horse program. This bit of cyberespionage quite possibly changed the course of events in the roiling Middle East.

Now able to monitor his communications and scan the data on the Syrian’s laptop, the Israelis scoured the hard drive and discovered a photograph of two men, one Asian, one Arab, standing in the Syrian desert. The Mossad was able to identify the men clearly: one was Chon Chibu, leader of the North Korean nuclear program, and the other was Ibrahim Othman, director of the Syrian atomic energy agency. With that photo and other documents on the laptop that revealed construction plans and photos of a pipe used for work on fissile material, the Israelis had clear evidence that the Syrians were secretly constructing a facility at al Kibar to process plutonium, a key step in the development of a nuclear bomb.

Armed with this information, the Israelis launched “Operation Orchard.” On Sept. 6, 2007, seven Israeli F-15I fighter jets flew into Syrian airspace in the dead of night. The jets dropped several bombs and destroyed the Kibar nuclear reactor site and flew home to Israel without a shot being fired at the planes. The Israelis, it turned out, had penetrated the Syrian military’s computer networks and were able to “spoof” the Syrian air defense operators with false information, thus foiling any radar detection of their jets. What well might have provoked a war in the region was met with silence by both sides. Rather than condemn the action, the Syrians hurriedly cleaned up the rubble and constructed another building to cover up whatever they had been doing.

According to a new book called Cybersecurity and Cyberwar: What Everyone Needs to Know by P.W. Singer and Allan Friedman, directors at the Brookings Institution, Operation Orchard is one example of the face of cyberwar in a world where technology has changed nearly all the rules of engagement.

The authors point out that this new type of warfare “has much in common with war as it has always been conducted. The computer used as a military weapon is just a tool.” But there is a major difference between current cyberespionage and past intelligence collection programs. Now, “computer network operations also allow aggressive actions inside the enemy’s communications once the shooting has begun. It’s the
The difference between reading the enemy’s radio signals and being able to seize control of the radio itself.”

Given the steady march of technology over the past three decades, among the most glaring ironies of this digitized world is the continued misunderstanding of cyberspace and cybersecurity. The authors quote Gen. Michael Hayden, a former CIA director, who said, “Rarely has something been so important and so talked about with less and less clarity and less apparent understanding.”

According to Singer and Friedman, the Pentagon, for example, has “issued at least 12 different definitions of what it thinks of as cyberspace.” Needless to say, such confusion sets off alarm bells for a global environment in which computers are so integral to every aspect of the lives of every inhabitant of the planet. Starting with the rash of hackers that emerged over the past 30 years to wreak havoc with random, targeted invasions of corporate, military and government computer systems, cybersecurity has long been a major concern.

Yet despite this anxiety, the authors point out, there has been a growing lack of understanding of the specific implications of cybersecurity and cyberwar, a dearth of knowledge and ideas that bodes ill for a world where technology is now the “critical infrastructure” of our lives. Putting up an effective battle against those who see the invasion and corruption of these systems as their means to do widespread harm requires a strong, working knowledge of cyberspace.

To this end, Singer and Friedman’s book is a must read, and lucky for all of us, it is a good read, a well-written and frighteningly clear primer that ought to be required reading in every boardroom and military situation room.

Unfortunately, the digitization of society has left a blind spot: we are nearly totally dependent on cyberspace for work, play, communications, safety and knowledge. But any mention of cybersecurity causes most users’ eyes to glaze over.

How many of us bother to change our passwords as often as the security experts recommend?

Everyone has experienced a technology meltdown at some point in their lives and most of us have been attacked by nasty and confounding viruses that spread like swine flu around the world at super speed. At those moments, we get a brief and chilling idea of what a major, orchestrated cyberattack might mean.

What Singer and Friedman do so well is put clarity around “the fog of war” that is cybersecurity and cyberwar. Those bracing for a cyber-9/11 or cyber-Pearl Harbor are waiting for the wrong kind of attack. The true nature of digital vulnerability in our world is far more subtle and sustained, “death by a thousand cuts” rather than a vast invasion that will knock out an entire nation’s technology infrastructure. The authors quote Dmitri Alperovitch, a threat researcher at the antivirus software vendor McAfee. “I divide the entire set of Fortune Globe 2000 firms into two categories,” Alperovitch said, “those that know they’ve been compromised and those that don’t yet know.”

www.cybersecuritybook.com