New York Times

June 3, 2012

IT took years after the United States dropped the atomic bomb on Hiroshima for the nation to develop a common national understanding of when and how to use a weapon of such magnitude. Not until after the Cuban Missile Crisis, 50 years ago this October, did a consensus emerge that the weapon was too terrible ever to employ again, save as a deterrent and a weapon of last resort.

Over the past decade, on a far smaller scale, the country's military and intelligence leadership have gone through a parallel debate about how to use the Predator drone. Because it is precisely targeted, often on an individual, it is used almost every week.

And now we know that President Obama, for the past three years, has been going through a similar process about how America should use another innovative weapon -- one whose destructive powers are only beginning to be understood. In a secret program called ''Olympic Games,'' which dates from the last years of the George W. Bush administration, the United States has mounted repeated attacks with the most sophisticated cyberweapons ever developed. Like drones, these weapons cross national boundaries at will; in the case of Olympic Games they invaded the computer controllers that run Iran's nuclear centrifuges, spinning them wildly out of control.

How effective they have been is open to debate; the United States and its close partner in the attacks, Israel, used the weapons as an alternative to a potentially far more deadly, but perhaps less effective, bombing attack from the air. But precisely because the United States refuses to talk about its new cyberarsenal, there has never been a real debate in the United States about when and how to use cyberweapons.

President Obama raised many of the issues in the closed sanctum of the Situation Room, participants in the conversation say, pressing aides to make sure that the attacks were narrowly focused so that they did not take out Iranian hospitals or power plants and were directed only at the country's nuclear infrastructure. ''He was enormously focused on avoiding collateral damage,'' one official said, comparing the arguments over using cyberwar to the debates about when to use drones.

Does the United States want to legitimize the use of cyberweapons as a covert tool? Or is it something we want to hold in reserve for extreme cases? Will we reach the point -- as we did with chemical weapons, and the rest of the world did with land mines -- that we want treaties to ban their use? Or is that exactly the wrong analogy, in a world in which young hackers, maybe working on their own or maybe hired by the Chinese People's Liberation Army or the Russian mob, can launch attacks themselves?

These are all fascinating questions that the Obama administration resolutely refuses to discuss in public. ''They approached the Iran issue very, very pragmatically,'' one official involved in the discussions over Olympic Games told me. No one, he said, ''wanted to engage, at least not yet, in the much deeper, broader debate about the criteria for when we use these kinds of weapons and what message it sends to the rest of the world.''

Cyberweapons, of course, have neither the precision of a drone nor the immediate, horrifying destructive power of the Bomb. Most of the time, cyberwar seems cool and bloodless, computers attacking computers. Often that is the case.

The Chinese are believed to attack America's computer systems daily, but mostly to scoop up corporate and Pentagon secrets. (Mr. Obama, one aide said, got a quick lesson in the scope of the problem when an attack on his 2008 campaign's computers was traced back to China, a foretaste of what happened to Google the following year.) The United States often does the same: the Iranians reported last week that they had been hit by another cyberattack, called ''Flame,'' that appeared to harvest data from selected laptop computers, presumably those of Iranian leaders and scientists. Its origins are unclear.

But the cutting edge of cyberwar is in the invasion of computer systems to manipulate the machinery that keeps the country going -- exactly what the United States was doing to those Iranian centrifuges as it ran Olympic Games. ''Somebody has crossed the Rubicon,'' Gen. Michael V. Hayden, the former director of the C.I.A., said in describing the success of the cyberattacks on Iran. General Hayden was careful not to say what role the United States played, but he added: ''We've got a legion on the other side of the river now. I don't want to pretend it's the same effect, but in one sense at least, it's August 1945,'' the month that the world first saw the capabilities of a new weapon, dropped over Hiroshima and Nagasaki.

That was deliberate overstatement, of course: the United States crashed a few hundred centrifuges at Natanz, it did not vaporize the place. But his point that we are entering a new era in cyberattacks is one the administration itself is trying to make as it ramps up American defenses. Defense Secretary Leon E. Panetta -- a key player in the Iran attacks -- warned last year that the ''next Pearl Harbor we confront could very well be a cyberattack that cripples our power systems, our grid, our security systems, our financial systems.''

IN March the White House invited all the members of the Senate to a classified simulation on Capitol Hill demonstrating what might happen if a dedicated hacker -- or an enemy state -- decided to turn off the lights in New York City. In the simulation, a worker for the power company clicked on what he thought was an e-mail from a friend; that ''spear phishing'' attack started a cascade of calamities in which the cyberinvader made his way into the computer systems that run New York's electric grid. The city was plunged into darkness; no one could find the problem, much less fix it. Chaos, and deaths, followed.

The administration ran the demonstration -- which was far more watered-down than the Pentagon's own cyberwar games -- to press Congress to pass a bill that would allow a degree of federal control over protecting the computer networks that run America's most vulnerable infrastructure. The real lesson of the simulation was never discussed: cyberoffense has outpaced the search for a deterrent, something roughly equivalent to the cold-war-era concept of mutually assured destruction. There was something simple to that concept: If you take out New York, I take out Moscow.

But there is nothing so simple about cyberattacks. Usually it is unclear where they come from. That makes deterrence extraordinarily difficult. Moreover, a good deterrence ''has to be credible,'' said Joseph S. Nye, the Harvard strategist who has written the deepest analysis yet of what lessons from the atomic age apply to cyberwar. ''If an attack from China gets inside the American government's computer systems, we're not likely to turn off the lights in Beijing.'' Professor Nye calls for creating ''a high cost'' for an attacker, perhaps by naming and shaming.

Deterrence may also depend on how America chooses to use its cyberweapons in the future. Will it be more like the Predator, a tool the president has embraced? That would send a clear warning that the United States was ready and willing to act. But as President Obama warned his own aides during the secret debates over Olympic Games, it also invites retaliatory strikes, with cyberweapons that are already proliferating. In fact, one country recently announced that it was creating a new elite ''Cybercorps'' as part of its military. The announcement came from Tehran.