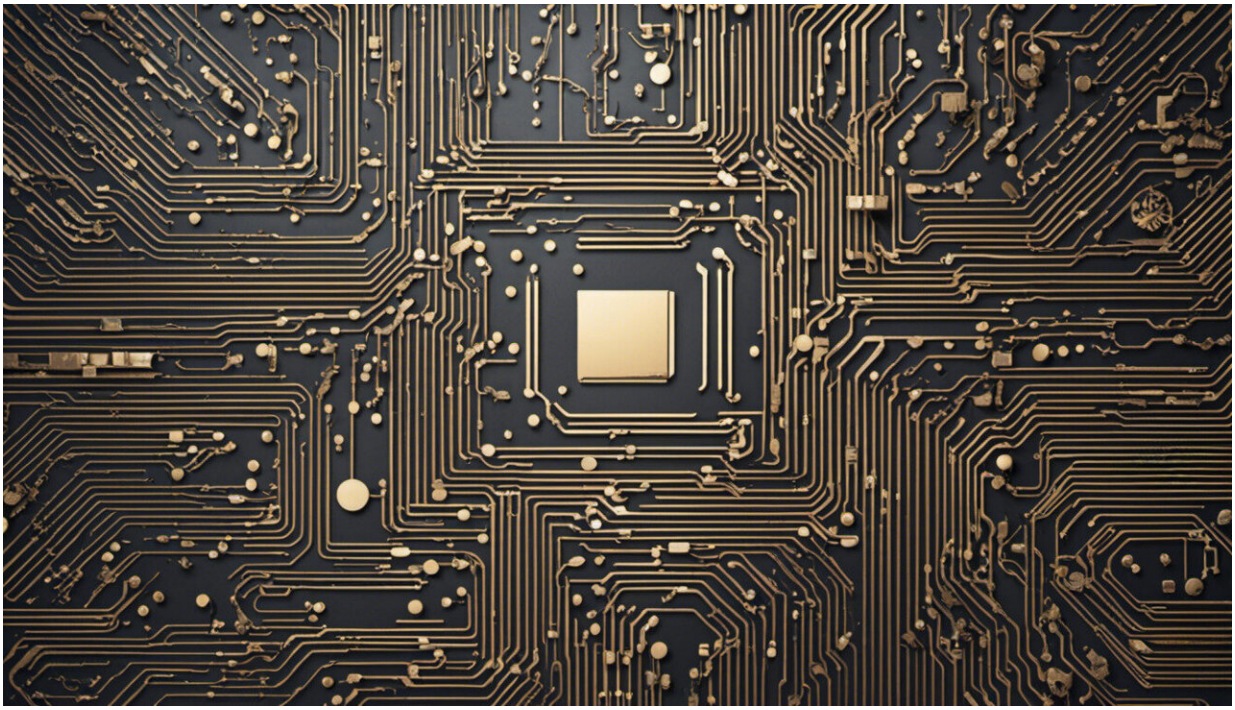
Cyberwar is here to stay

February 24 2016, by Paul Rosenzweig, George Washington University



Credit: AI-generated image (disclaimer)

Last week, *The New York Times* revealed that the Obama administration had prepared a cyberattack plan to be carried out against Iran in the event diplomatic negotiations failed to limit that country's nuclear weapons development.

The plan, code-named Nitro Zeus, was said to be capable of disabling Iran's air defenses, communications system and parts of its electric grid.

It also included an option to introduce a computer worm into the Iranian uranium enrichment facility at Fordow, to disrupt the creation of nuclear weapons. In anticipation of the need, U.S. Cyber Command placed hidden computer code in Iranian computer networks. According to *The New York Times*, President Obama saw Nitro Zeus as an option for confronting Iran that was "short of a full-scale war."

The reports, if true (to be fair, they have not been confirmed by any official sources), reflect a growing trend in the use of computers and networks to conduct military activity.

The United States is not, of course, the only practitioner. One notable example from recent history involves the apparent Russian assault on the transportation and electric grid in Ukraine. That attack, which happened late in 2015, was a "first of its kind" cyberassault that severely disrupted Ukraine's power system, affecting many innocent Ukrainian civilians. It bears noting that the vulnerabilities in Ukraine's power system are not unique – they exist in power grids across the globe, including the U.S. power grid and other major industrial facilities.

Built-in vulnerabilities

The vulnerability of digital networks is, in many ways, an inevitable consequence of how the Internet was built. As then-Deputy Secretary of Defense William Lynn put it in a 2011 speech announcing our military strategy for operating in cyberspace: "The Internet was designed to be open, transparent and interoperable. Security and identity management were secondary objectives in system design. This lower emphasis on security in the internet's initial design … gives attackers a built-in advantage."

Among many factors, two in particular contribute to the growing sense of unease.

One is the problem of anonymity. Those who seek to do harm can easily do so at a distance, cloaked in the veil of anonymity behind false or shielded identities in the vastness of the web. With no built-in identity verification, pretending to be someone else is as easy as getting a new email address or registering a pseudonymous Facebook account.

Unmasking attackers is possible, but requires a significant investment of time and resources. It also often requires the "good guys" to use "bad guy" techniques to track the malefactors, because they need to hack the hackers to find out who they are. It took a Canadian company, using hacker techniques, more than a year to find out who had hacked the Dalai Lama's official computers – it was the Chinese.

In effect, this prevents targets from retaliating against attackers. Though most observers think Russia is behind the Ukrainian assault, there is no truly conclusive proof. It is very difficult to deter an unknown attacker. In addition, international coordination to respond to attacks that threaten global stability can be stymied without solid proof of the source of an assault.

A new definition of war

Second, and perhaps more significantly, the online world changes the boundaries of war. President Obama seems to think that cyberattacks are less than full-scale war (or so the *Times* reports). Is that realistic? Consider the following hypotheticals – all of which are reasonably plausible.

An adversary of the United States (known or unknown):

- Disrupts the stock exchanges for two days, preventing any trading;
- Uses a digital attack to take offline a radar system intended to

provide early warning of an aerial attack on America;
- Steals the plans to the F-35 fighter;
- Disrupts the Pentagon's communication system;Introduces a latent piece of malware (a piece of malicious software that can be activated at a later date, sometimes called a "logic bomb") into a radar station that can disable the station when triggered, but doesn't trigger it just yet;
- Makes a nuclear centrifuge run poorly in a nuclear production plant, eventually causing physical damage to the centrifuge; or
- Implants a worm that slowly corrupts and degrades data on which certain military applications rely (such as GPS location data).

Some acts, like stealing the plans for a new fighter jet, won't be considered acts of war. Others, like disrupting our military command and control systems, look just like what we have always thought of as acts of war.

Introducing uncertainty

But what about the middle ground? Is leaving a logic bomb behind in a radar station like espionage, or is it similar to planting a mine in another country's harbor as a preparation for war? What about the computer code Nitro Zeus allegedly placed in the Iranian electric grid? And what if that code is still there?

These are hard questions. And they will endure. The very structures that make the Internet such a powerful engine for social activity and that have allowed its explosive, world-altering growth are also the factors that give rise to the vulnerabilities in the network. We could eliminate anonymity and restrict the potential for digital attacks, but only at the price of changing the ease with which peaceful people can use the Internet for novel commercial and social functions.

Those who want both ubiquity and security are asking to have their cake and eat it, too. So long as this Internet is "The Internet," vulnerability is here to stay. It can be managed, but it can't be eliminated. And that means that those who bear responsibility for defending the network have a persistent challenge of great complexity.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation