In recent months the role of powerful US-based transnational tech corporations has taken center stage. From censoring national leaders to purging entire political movements and discussions from their platforms, never has the power to influence what people can say, see, and hear been held in so few hands.

Beyond this threat is a new form of information warfare where nations like the United States are able to enter into and dominate the information (or cyberspace) of a targeted nation, both by controlling traditional media, but also by using networks controlled by US-based social media corporations manipulate public perception, promote particular political agendas and silence critics of US foreign policy and interests. The US-engineered "Arab Spring" in 2011 was a dramatic example of how this type of information warfare could be used to help pave the way for more traditional (and more destructive) forms of warfare.

Today, we are seeing entire conflicts play out online where not only influence is being sought - but entire nations are being cut-off, silenced, or otherwise impacted.

**The Need to Defend Cyberspace**

In the 29th century, a nation needed an army to protect its borders and a navy to protect its shores. In the 20th century, with the invention of the airplane, air forces were required to protect this new frontier of warfare, a nation's
Today the importance of cyberspace for communication, business and governance cannot be argued. But there appears to be a lag throughout the world in understanding the importance of this new frontier and the need to protect it just as vigorously as a nation protects its borders, shores and airspace.

However, there are a few exceptions. The US clearly understands the potential threats to its own cyberspace since it is the primary threat to the cyberspace of nations globally.

Nations like China and Russia have led the way in developing alternatives to US-based social media networks that have been weaponized and work hand-in-hand with the US government in executing foreign policy.

Both nations also have protections about what sort of information can and cannot flow in and out of their borders, with China having clearly the most formidable defense in this respect.

More recently, Russia has announced its ability to shut itself off from the wider, US-dominated Internet under extreme circumstances.

Russian state media would report in an article titled, "Russia has plan to cut off country from ‘US-controlled’ global internet, but only as ‘last resort,’ says former President Medvedev," that:

Former President Dmitry Medvedev, now deputy chairman of the country’s Security Council, told local media on Monday that, as a drastic last resort, Russia could cut off access to servers beyond its borders. According to him, with the way the internet is currently set up, “the key rights to control are in the United States of America.”

The article would also note:

In recent years, Russia has made significant investments in developing its domestic online infrastructure, and Medvedev pointed to regulations that would allow the country to limit the web to its own autonomous networks. The politician was at pains to emphasize that these plans were contingencies, and that Russia would “really not want to” shut itself off from the digital world.

In many ways, developing a nation's domestic online infrastructure and ensuring independence especially during a crisis is similar to establishing well-controlled borders within the physical world. They are not borders any nation would ideally want to close or control too strictly, but having the ability to defend them when under attack is clearly a necessity.

Russia's example is an example other nations should be taking to heart. Nations should also note the success Russia and China have had in defending their respective nations and interests within information space and cyberspace.

A nation today without defenses for these new frontiers of social, economic and now military activity are like nations in the 20th century without air forces, or nations in the 19th century without standing armies and capable navies. Such nations open themselves up for "virtual" invasions and the disruption and destabilization of both political and economic activity.

Examples of this are rife around the globe where US-backed regime change is now always accompanied by attacks on and invasions of a targeted nation's information space and cyberspace. Lessons are being learned the hard way that even small nations need to build up their own infrastructure as well as social media networks to fill up their respective spaces before an adversary does.

Historically, those who control the lines of communication held a distinct, even pivotal advantage upon the battlefield. Today, these "lines" are now entire spaces permeating virtually every aspect of daily life.

Considering all of this, nations that still do not take this threat seriously and do not define and then pursue the defense of their national information space and cyberspace place themselves, their people and their future in grave peril.

Ulson Gunnar, a New York-based geopolitical analyst and writer especially for the online magazine “New Eastern Outlook”.
