GlobalResearch
Center for Research on Globalization

US Seeks to Monopolize Cyberwarfare

By Ulson Gunnar
Global Research, September 17, 2017
New Eastern Outlook 15 September 2017

Region: USA
Theme: Intelligence, Police State & Civil Rights, US NATO War Agenda

The use of information to enhance martial power goes back to the beginning of human civilization itself, where propaganda and psychological warfare went hand-in-hand with slings, arrows, swords and shields.

The most recent iteration of this takes the form of social media and cyberwarfare where tools are being developed and deployed to influence populations at home and abroad, to manipulate political processes of foreign states and even tap into and exploit global economic forces.

In the beginning of the 21st century, the United States held an uncontested monopoly over the tools of cyberwarfare. Today, this is changing quickly, presenting an increasingly balanced cyberscape where nations are able to defend themselves on near parity with America's ability to attack them.

To reassert America's control over information and the technology used to broker it, Jared Cohen, current Google employee and former US State Department staff, has proposed a US-created and dominated "international" framework regarding cyberconflict.

His op-ed in the New York Times titled, "How to Prevent a Cyberwar," begins by admitting the very pretext the US is using to expand its control over cyberwarfare is baseless, noting that *"specifics of Russia's interference in the 2016 America election remain unclear."*

Regardless, Cohen continues by laying out a plan for reasserting American control over cyberwarfare anyway, by claiming:

> Cyberweapons won't go away and their spread can't be controlled. Instead, as we've done for other destructive technologies, the world needs to establish a set of principles to determine the proper conduct of governments regarding cyberconflict. They would dictate how to properly attribute cyberattacks, so that we know with confidence who is responsible, and they would guide how countries should respond.

Cohen, unsurprisingly, nominates the US to lead and direct these efforts:

> The United States is uniquely positioned to lead this effort and point the world toward a goal of an enforceable cyberwarfare treaty. Many of the institutions that would be instrumental in informing these principles are based in the United States, including research universities and the technology industry. Part of this effort would involve leading by example, and the United States can and should establish itself as a defender of a free and open internet everywhere.

Cohen never explains how this US-dominated framework will differ from existing "international" frameworks regarding conventional warfare the US regularly abuses to justify a growing collection of devastating conflicts it is waging worldwide.

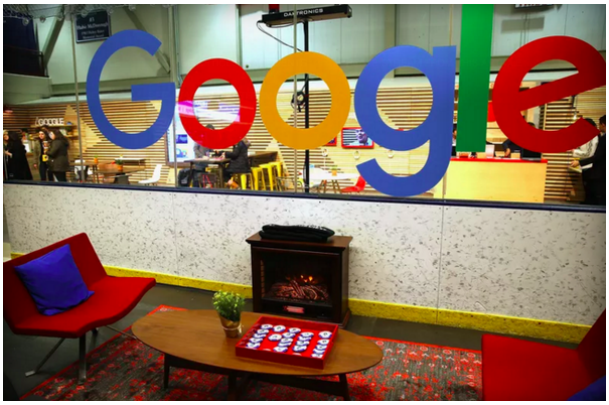
And as has been repeatedly documented, the United States' definition of a *"free and open internet everywhere"* is an Internet dominated by US tech companies seeking to enhance and expand US interests globally.

Cohen ironically notes that:

> Cyberweapons have already been used by governments to interfere with elections, steal billions of dollars, harm critical infrastructure, censor the press, manipulate public conversations about crucial issues and harass dissidents and journalists. The intensity of cyberconflict around the world is increasing, and the tools are becoming cheaper and more readily available.

Indeed, cyberweapons have already been used, primarily by the United States.

Jared Cohen himself was directly involved in joint operations between Google, Facebook, the US State Department and a number of other US tech and media enterprises which before and during 2011 set the stage for the so-called "Arab Spring."



It included the training, funding and equipping of activists years ahead of the the uprisings

as well as active participation in the uprisings themselves, including providing assistance to both protesters and militants everywhere from Libya to Syria in overthrowing governments targeted by Washington for regime change.

One such tool used in these efforts was described in a UK Independent article titled, "Google planned to help Syrian rebels bring down Assad regime, leaked Hillary Clinton emails claim," which would report that:

> An interactive tool created by Google was designed to encourage Syrian rebels and help bring down the Assad regime, Hillary Clinton's leaked emails have reportedly revealed.
>
> By tracking and mapping defections within the Syrian leadership, it was reportedly designed to encourage more people to defect and 'give confidence' to the rebel opposition.

The article would continue, mentioning Jared Cohen by name:

> The email detailing Google's defection tracker purportedly came from Jared Cohen, a Clinton advisor until 2010 and now-President of Jigsaw, formerly known as Google Ideas, the company's New York-based policy think tank.
>
> In a July 2012 email to members of Clinton's team, which the WikiLeaks release alleges was later forwarded to the Secretary of State herself, Cohen reportedly said: "My team is planning to launch a tool on Sunday that will publicly track and map the defections in Syria and which parts of the government they are coming from."

Would Cohen's more recently proposed "framework" have prevented the United States' use of these cyberweapons against sovereign states to undermine sociopolitical stability, overturn entire governments and plunge them into enduring chaos many still remain in 6 years later? Most likely not.

What Cohen and the interests he represents are truly concerned with is that nations are now not only able to recognize, prepare for and defend against US cyberwarfare, they may be capable of retaliating against the US.

Cohen's proposal for an international framework to govern cyberwarfare simply seeks to define it in terms that leaves the US with both an uncontested monopoly over cyberwarfare as well as the means to wield it globally with absolute impunity.

It would be not unlike current "international" frameworks used to govern conflicts between nations which the US has used to justify an expansive, global campaign of extraterritorial war stretching from North Africa to Central Asia and beyond.

Such frameworks have become enablers of injustice, not a deterrence to it.

As nations from Iran to North Korea are discovering, the only true means of defending oneself from foreign military aggression is creating a plausible deterrence to dissuade foreign nations from attacking. This is done by creating a price for attacking and invading

that is higher than the perceived benefits of doing so.

Nations like Russia and China have already achieved this balance with the United States in terms of conventional and nuclear warfare, and have now nearly established a similar deterrence in terms of cyber and information warfare. For the rest of the world, developing cyberdefense is not as costly as conventional military or nuclear arsenals, making cyberwarfare a corner of the battlefield unlikely to be monopolized by the US as it had done at the turn of the century.

Ensuring that no single nation ever has the opportunity to abuse such a monopoly again means exposing and confronting efforts by those like Google's Jared Cohen and his proposal for an "international framework" for cyberwarfare that resembles the same sort of enabling the United Nations provides the US in terms of proliferating conventional conflicts across the globe.

Ulson Gunnar is a New York-based geopolitical analyst and writer especially for the online magazine "New Eastern Outlook".

All images in this article are from New Eastern Outlook.

Articles by: Ulson Gunnar