World War III is being waged in cyberspace

October 5 2017, by Dr. Mike Sosteric

Credit: AI-generated image ([disclaimer](link))

My introduction to advanced communication technology (i.e. the Internet and World Wide Web) came in 1999.

Having grown up in the two-channel universe of the 1960s and '70s, I was agog at the power it represented. The technology was nascent at that time—not many web pages yet existed—but I could still see the potential for good. Here was a technology that I felt could really save the world.

I am not ashamed to say that when I first saw the Web, I was filled with schoolboy naivete. I wanted to help, so I did. I created the first electronic sociology journal, [did a few more things after that](), and with a massive anticipatory grin, watched and waited for utopia.

Unfortunately, utopia didn't emerge. In fact, my naive grin soon melted away.

The melting began when I learned that researchers at Cornell University, [working without ethical oversight]() and possibly in collusion [with the U.S. Department of Defense](), were learning how to use Facebook, a technology we keep by our beds, [to manipulate mass emotion]().

The grin melted even further when I saw fellow scientists had learned to [use search engines to manipulate political preferences]().

Manipulating Trump supporters

The grin turned to an outright frown when I read [in that same study]() by the *Proceedings of the National Academy of Sciences*, a multidisciplinary scientific journal, that moderate Republicans, moderate libertarians, male Republicans and the "deplorable" poor—President Donald Trump's base—were the most susceptible to manipulation.

I became a little worried when the scholars who wrote the study suggested that Google, by manipulating its algorithms, [might already have decided a foreign election, in India in 2014](), in favour of a right-wing candidate.

Then there was the historic 2016 election of Trump. That's when my smile turned to a grimace. During that election campaign, Trump [called out to Russia to hack the election](), which they did. Spewing hundreds of thousands of dollars of fake ads into [Facebook](), [Twitter]() and probably

[Google](#), they attacked America full-on. They didn't do it with bullets and bombs; they did it with [bits](#) and with [bytes](#), and with the help of American CEOs and American technology.

It was certainly an attack, and there were definitely explosions, but they were in cyberspace. Desensitized by Hollywood violence, we are not paying attention to the attack on our minds.

You can argue about whether the Russian attacks were effective, or puzzle if Trump and his family are traitors, but the fact remains—we are under attack, and if something isn't done, it's going to get worse.

Annual hacking event

You don't have to be a prophet to see what's coming. The battle plan is in plain sight.

Consider the Russian company [Positive Technologies](#). This firm holds an annual event known as [PHDays](#), or "Positive Hack" days. At this event, which started back in 2011, the world's best and brightest hackers get together to train.

It doesn't sound too threatening until you learn about "[The Standoff](#)." The Standoff is a military hacking competition with a blatant military goal: Take out a city's telecom, heat, power, oil, and rail infrastructures. The city's citizens are even offered up as a resource for the hackers. They are easy to exploit, [says the rule book](#). They use "smart gadgets every day." "They are vulnerable to social engineering." They are "prepared to share [their] secrets."

> Critical infrastructure at [#PHDays](#)
> [pic.twitter.com/DUgE7n2RKk](#)

— Positive Hack Days (@phdays) [May 24, 2017](link)

Sitting back in my chair with a thump, I see it clearly.

There's a global war going on, and a global arms race to go with it. The arms race is not a race for physical weapons, it is a race to develop cyber-weapons of psychological, emotional, financial and infrastructure attack. By now, the [arms race](link) is so far advanced that it makes the [leaflet campaigns of the Second World War](link) and the U.S. government's [Operation Cornflake](link) look like toddler's play.

[ISIS](link) and the [far-right are using Twitter](link) and other [online networks](link) to radicalize our youth, bringing the war to our streets. Russian cyber-marines [engage in massive cyber-attacks](link), going so far as to target [our voting machines](link).

Just recently, the sensitive financial data of almost half the U.S. population was stolen by [state-sponsored professionals](link). There is even, as is becoming increasingly clear as the [Meuller investigation into Trump's Russia connections](link) unfolds, a "[highly coordinateed disinformation campaign](link)"—a propaganda campaign, [aimed at destabilizing American society](link).

Wake up and realize we're at war

If the horrific [recent gun violence in Las Vegas](link), exploding racial tensions and political polarization of Western democracies are any indication, destabilization is proceeding apace.

So what do we make of this?

No. 1: Realize that global war has been declared. It's a little hard to pin down who fired the first shot right now, but the aggressors are active and

engaged.

No. 2: Understand we are all under attack, even Republicans, [perhaps especially Republicans, and the poor.](#) There may be short-term financial gain for those who benefit from the destabilization, but only a fool would think the enemy is our best friend.

Finally, if you are a private citizen, you need to start taking the cyber threat seriously. Combatants are trained to see you as easy-to-manipulate resources. You are being viciously manipulated through social media.

Your [financial data](#) is stolen and could easily be used against you. Cyber-marines are training to take out the life-giving infrastructure of your cities. Are government and corporate leaders blithely unaware, or engaged in traitorous collusion? Only time will time.

Until then, wake up, gather your loved ones, lock down your social media, and batten the hatches—the war for your mind has begun.

This article was originally published on [The Conversation](#). Read the [original article](#).

Provided by The Conversation