A war within a war: Cyberattacks signal a new, powerful approach to combat

March 3 2022, by Claire Hall

Credit: Pixabay/CC0 Public Domain

Over the past few days, the Russian invasion of Ukraine has captivated the attention of the world. But in addition to fighting with troops on the ground, the nation is also defending itself on another front, from

cyberattack.

This "war within a war" is another strategy used by Russia to disrupt and disable life in Ukraine and increase that nation's vulnerability. But the attacks aren't confined just to two nations. The ripple effects can be seen around the world. In fact, Ukrainian leaders have asked international cyber experts to help them create an "IT Army" to protect it from harm.

Professor Stephen Fitzgerald of the Operations and Information Management Department at the School of Business has closely monitored the cyber threats in Ukraine. He says the attacks and counterattacks are something the U.S., too, should follow closely.

What role have cyberattacks played in the assault in Ukraine?

Similar to the Colonial Pipeline attack targeting U.S. fuel infrastructure, many of the attacks are made with the intent to cripple the Ukrainian war effort by sabotaging communications, agriculture, commerce, supply lines, machinery, finance and energy.

It is hard to say how easy infiltration is; it depends on the system and the attack. But it is worth noting that the attacks being launched are quite sophisticated, and we can't overlook the inherent power imbalance between the two countries playing a role.

In response, many companies and nations have sanctioned Russia's access and assets online.

Additionally, capable groups and vigilantes from all over the world, including the infamous hacktivists of Anonymous, have come to the defense of Ukraine by attacking Russia back. Claiming credit for

multiple attacks, the collective has disabled a Russian news site, and released emails and passwords from the Russian Ministry of Defense.

While this impressive effort seems like a win, we must remain cognizant that we are only getting a tiny fraction of the picture. Leaked passwords are useless once published, and the RT news site appears to be back up and running. We continue to gather as much information as we can on the cyber war being raged, but the truly devastating or dangerous attacks we may never know about. As a part of the outbreak of war, cyberattacks have occurred in shocking speed.

How is Ukraine responding to this cyber assault?

To aid in their cyber defense, Ukrainian Vice Prime Minister Mykhailo Fedorov has posted a Tweet asking for volunteers to fight on the digital front, solidifying the conflict as a 21st century war. It has been said that future wars will not be fought on the ground, but online. While this is not the present case, we may be witnessing the first formalized iterations of such future conflicts.

Traditionally, cyberwarfare has been an unspoken constant, with governments claiming plausible deniability or pointing the finger at criminal organizations who inhabit their country as they posture against one another. It has historically been hard to prove a nation state's culpability in cyberattacks, but now that there is open warfare in Europe, there is no need to be clandestine and both sides can attack and defend with their full capabilities.

How will this online war impact the United States?

This is a tough question to answer because there is currently so much uncertainty. While the U.S. is physically distant from the fighting,

cyberwarfare is not constrained by distance. Some say President Biden has been pressured to take action on Russia, many of which include cyber attacks of our own to disrupt Russian internet connectivity, electrical power, and transportation.

Of course, this invites a retaliatory effort from our historic adversary which should give officials appropriate pause. It is completely reasonable to expect that whatever we can do to Russia, they can do to us. The U.S. does not want open cyber conflict with Russia and an actual cyber attack from the U.S. is almost completely off the table from what is being discussed, according to the White House.

This back and forth highlights just how tricky the situation is and how hard it is to pin down reliable information. One concern that we can cite for certain is the idea that the software programs used in these attacks could spill over or cause collateral damage based on their design.

How vulnerable is the U.S. to similar attacks?

It is unlikely that individual Americans will be targeted by attacks, but if we were to see conflict we would likely see attacks that target valuable infrastructure or specific corporations.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has made a point to warn Americans about some of the malware we have seen coming out of the conflict, and have taken on the mantra "Shields Up" to describe our nation's cyber defense posture.

"While there are no specific or credible cyber threats to the U.S. homeland at this time, Russia's unprovoked attack on Ukraine, which has involved cyber-attacks on Ukrainian government and critical infrastructure organizations, may impact organizations both within and beyond the region, particularly in the wake of sanctions imposed by the

United States and our Allies. Every organization—large and small—must be prepared to respond to disruptive cyber activity," CISA said in a statement.

In the meantime CISA has published a page describing some of the steps and resources individuals and companies can use to protect themselves from any sort of online shrapnel. As with all cybersecurity risks, the best thing we can do is to proactively prepare and have a plan if we are to be attacked.

How might the international community address these aggressions?

Microsoft, which has for some time called for the creation of a new Geneva Convention pact governing cyberspace, is now suggesting that some cyberattacks on Ukraine could be considered war crimes under existing international laws. This is certainly something the international community will need to address at some point in the near future. Although international cyberlaw is in its infancy, it will need to quickly mature as the international community deals with the ongoing wartime cyberattacks.

Provided by University of Connecticut