# The World Needs A 21st Century Arsenal of Democracy

This article was originally published on Fox Business on May 15, 2014.

*by Brian E. Finch*

**Brian E. Finch**
Public Policy
+1.202.663.8062
brian.finch@pillsburylaw.com

Brian E. Finch is a partner in Pillsbury's Public Policy practice in Washington, DC. He is a recognized authority on global security matters and is co-leader of the firm's Global Security practice.

Poland, Estonia, Latvia, and Lithuania cannot look back with much comfort on the promise of Western assistance in the face of military aggression.

France, after all, had agreed in the *1939 Kasprzycki-Gamelin Convention* to come to the aid of Poland in the event of an attack by Germany. True to form, the Française Armée de la République launched an invasion of Germany one week after its surprise invasion of Poland.

France's Saar offensive did not, however, represent the zenith of military daring. Instead, it involved a rather lackadaisical occupation of a few (abandoned) German villages, all of which were immediately abandoned when German troops reappeared in force.

It should be no surprise then Russian President Vladimir Putin's hostile adventures in Ukraine is inspiring great worry from our Eastern European allies. In order to dissuade the Russian bear from turning westward, the U.S. has deployed several fighter jets and 600 troops total to Poland, Estonia, Latvia, and Lithuania. Ukraine, meanwhile, is slated to receive a consignment of helmets, generators, and sleeping bags. One does not suspect that will alter Russia's strategic plans.

Such measures smack of little more than lip service to treaty commitments and ideals of territorial integrity. If America really wants to provide immediate and needed assistance to Russia's nervous neighbors — without provoking an open military conflict by the way — it needs to become a 21st century arsenal of democracy.

Russia is a cyber superpower and it has, at its disposal, a variety of advanced cyber weapons to use against any foe. There is no doubt that if aggressive moves are taken against Poland and the Baltic states, cyber shots will be amongst the first fired. Russia's military adventures over the past 15 years reveal that it is not in any way afraid to use cyberattacks to lash out at its friends and foes alike.

Take for example the cyberattacks that overwhelmed Estonia in early 2007. Almost overnight the websites of the Estonian parliament, various banks, government agencies, and news outlets came under electronic siege. All of this happened thanks to a dispute over the relocation of a Soviet-era war monument and some military graves. While the Kremlin never admitted responsibility for the attacks, most analysts agree it was, at the very least, the work of hackers operating with the

knowledge and consent of Russian officials. Similar attacks are alleged to have also occurred during Russia's brief invasion of Georgia, and more recently in the Ukraine.

Indeed, it is quite likely that numerous Russian-launched pieces of malware are already sitting on systems in Poland and the Baltic states. Such malware can be used for a multitude of purposes, ranging from nuisance-like denial of service attacks to disruption of critical infrastructure systems, including energy delivery and communications backbones.

We can feel confident then that Russia's neighbors are staring down the barrel of a digital rifle. In truth they likely are already under significant attack. Russian national security agencies and cyber irregulars are masters of preemptively deploying advanced cyber threats such as using previously unknown exploits or malware with constantly changing code to evade standard defenses against any nation it believes might be opposed to its goals and interests.

A much more meaningful move by the United States to demonstrate its determination to aid its friends then would be to deploy defensive cyber assets. The dispatch of advanced cyber defensive tools like next generation firewalls, behavioral-based malware detection systems, cyber analysts, and other weapons in the American cyber armory will have an immediate impact on the security posture of our friends in Poland and the Baltic states.

Given Russia's extremely advanced cyber warfare capabilities, it makes perfect sense for the U.S. to lend its cybersecurity capabilities to the imperiled states. While even American cybersecurity systems are not perfect, they are light years ahead of what is typically available, and so deploying those assets and support personnel will give a much needed defensive boost to our Eastern European friends.

Just as importantly, the deployment of defensive tools will also give the world community an important card to play with Putin: accountability. American cyber forensic capabilities are cutting edge, and the opportunity to monitor attacks in real time, as well as dissect existing malware, will counter the maskirovka Russia uses with regularity to hides its identity and intentions. The ability to definitively link cyber warfare with the Putin machine is certainly a card America should have in its hand.

Like it or not, America still is the global guardian of freedom and responsible international behavior. If we are to, in the words of Secretary of State John Kerry, respond to 19th century tactics with 21st century tools, let's do it the right way. Sharing cybersecurity assets with our threatened friends is the right place to start.