The success of Russia’s attacks and interference in the 2016 election are dangerous not just because of their impact, but also because of how they will serve as a guidepost to others in the future. Congress should redefine the institutions involved in our democracy as critical infrastructure, in order to provide higher levels of support from the federal government. Contrary to the approach so far, however, we must recognize that the critical infrastructure of elections is not just the voting machines, but also the wider ecosystem, including parties and campaigns. Much as banks compete, but still share threat information, our election systems and political organizations, including even both the RNC and DNC, should have had the structures to cooperate in this space. Indeed, the only thing that would have been necessary to stop the entire DNC hack was a better line of communication between the organization’s IT staff and the FBI agents who had been tracking the Russian hacking for years.

Our need for resilience extends beyond bits and bytes, though, to building up better political resistance to the influence operations that allows Russia to exploit its cyber attacks. We must continue to uphold our freedom of speech but also ensure that authoritarian leaders don’t take advantage of it. Congress should reconvene the Active Measures Working Group, an interagency effort during the Cold War that debunked the worst of Soviet misinformation. It should also work in cohesion with our NATO allies to help identify and counter Russia’s campaigns (many of which just pivoted from targeting US to European voters). This will also help in debunking the individuals and outlets who have chosen to become either willing partners or полезные дураки, “useful idiots,” for foreign government propaganda.

Other parts of society will also have to weigh their own roles, much as in the Cold War. Tech firms have too long looked away at the manipulation of their networks by extremist groups and now authoritarian governments. The activities by Russian troll factories and bot campaigns that accelerate false news and propaganda violate terms of service and should become a target of reform in social media.

So too does traditional media need to rethink how it rewards these campaigns. When hackers outed millions of people cheating on their spouses after the Ashley Madison breach, responsible journalists reported on the breach, but not the fruits of it. By contrast, they breathlessly reported the most minute and personal details in the latest Russian government attacks. The New York Times public editor even acknowledged last year that by acting this way, the paper had ended up functioning as a “a de facto instrument of Russian intelligence.”Will media continue to be so in the future?