

U.S. Sen. Mark R. Warner
Transcript
March 1, 2018

Thank you, Bill, thank you for that very kind introduction. It is great to see everyone here this morning. I recall a number of times in the last few weeks or few months that people have been kind enough to come up and say, you know, either to me or Richard Burr, gosh you guys, it's, it's so good, we're so happy that you're the adults in the room. And I think, what a low bar we've struck. Again, thank you Bill for that introduction, and boy oh boy I could use your steady hand at the State Department these days more than ever. I'm so glad that you're still engaged in the fight here, through this great platform you have at Carnegie. You've always been a clear and strategic thinker and on behalf of all of us who continue to serve in the day job, thank you for what you're doing. And as Bill mentioned, timely time to have this kind of presentation and the good work that Carnegie's doing.

I'm going to acknowledge my age and put on my glasses, but the speech that Mr. Putin made yesterday or earlier today indicates that his current status quo approach of being extraordinarily aggressive and bellicose on a series of fronts is not going to disappear.

So again, my kudos to Carnegie for their informative work on trying to decipher this extraordinarily complex U.S.-Russia relationship. Because, again, it's not a news flash—too often those of us who are caught up in the day-to-day, who's down in Washington, we're all caught up in the latest news cycle, and I'm concerned that we can miss how this failure to step back, how all of these events actually form a context, and are basically presenting themselves, and what I believe is an alarming picture, in a sense of the new Russia and how it's emerging as a threat to both the United States and our allies.

So, the chance for me to come today to step back and try to sort through some of the strategic and policy implications for our national security is very important, so again I thank you for the opportunity.

And, if we just think about for just a moment, even the terminology. Let me go down just some of the litany. Bots. Paid trolls. Click farms. Little green men. Distributed denial of service. In the last couple of years, national security leaders have been forced to learn a whole new language in terms of dealing with 21st century threats. Our long-standing rival, Russia, has clearly reemerged in the world and with a new playbook to exploit our very openness, and our society to divide us from within, and, cut us off from our allies.

Some commentators have tried to define this as a new phase of the Cold War, but what we're experiencing now, to me, doesn't resemble the Cold War that I recall growing up with. Back then, we had a clear sense of who our adversary was, and I think Americans clearly, across the board understood that threat.

It even had a physical form: The Berlin Wall, which divided East from West... capitalism from Communism... freedom from oppression. We all knew who the bad guys were, where they stood, and our national security because of those clear divisions strategically emanated from that.

Today's conflict, I believe, is much more amorphous. In addition to the traditional tools of the Cold War, Mr. Putin has at his disposal a wide array of non-conventional weapons and tools – tools like cyberattacks, energy deals, hacking, selective leaking, and a bot army to sow and spread disinformation.

These tools are all designed to help Russia undermine its enemies in the West, but they're often deployed—and this is again one of the distinctions between the phase conflict we are in now, versus the traditional Cold War—many of these tools are actually deployed by non-state surrogates, thereby giving Russia the ability to claim deniability when their hand, their agents are caught taking some of these actions.

The bottom line? I believe rather than a framework of an old Cold War, I believe we are now engaged in a “**Fight in the Shadows.**” And I'm not sure that's a fight that we're currently winning.

So again, let me take a moment to at least give my perspective on how we got here, and what we need to do on a going-forward basis.

After the Berlin Wall fell, the United States reached out to the so-called “new Russia” under then President Yeltsin and attempted to bring it into the western community of nations. We, perhaps naively, assumed that Russia's eventual integration into institutions like the G7 and the EU was both natural and inevitable. Many of us imagined- that after the failure of communism, the allure and success of western, free-market democracy would almost automatically spread eastward. At the same time, we watched Russia's conventional military atrophy and its economy stagnate. And frankly, I think across most of the foreign policy establishment, we assumed that the Russian threat was greatly reduced. Facing these changed times, we in effect, declared the Cold War was over, and that we had won.

We turned our focus from superpower rivalry to counterterrorism, obviously the wars in Iraq and Afghanistan, and the challenges emanating from failed states. We worked to track down, chase and finally kill and eliminate terrorists around the world. This was a logical and understandable transformation, given the 9/11 attack, and other threats to our security emanating from the increasing number of failed states around the world. However, there was a cost to these decisions—and we took our eyes off the re-emerging threat posed by Russia.

What we did not imagine at the time—and perhaps we should have—was the resentment that many Russians felt at the economic uncertainties of the new free market... the chaos and inflation that wiped out many Russians' permanent savings. We failed to recognize, and I think, adequately predict, the corruption of a small, growing clique of oligarchs... and I think we failed

to understand the kind of psychic hit that most Russians felt with the loss of the superpower status that the Soviet Union had.

These feelings led directly into ordinary Russians' desire for stability and frankly their disenchantment with that very short-term Russian experiment with real democracy. All this ultimately led to a further enhancement and entrenchment of President Putin's power.

Meanwhile, as we saw in yesterday's speech, and as we've seen throughout his comments over the last few years Putin continued to nurse a grudge against the West. He called the demise of the Soviet Union the "greatest geopolitical catastrophe of the century." He used his growing control of television, film, and other organs of propaganda as a way to stoke popular discontent, and to further encourage ordinary Russians' disillusionment.

Putin relied on these powers to boost his standing with the Russian public and in a sense to replace the old notion of a Russian-led, communism-based philosophy with a whole new sense of 21st century Russian nationalism. And... with that backing of the vast majority of his public, he began an ambitious program of rearmament—all with the aim, I believe, of challenging the United States and our allies.

So, while our gaze shifted away from Russia—which we began to kind of write off and on a certain level dismiss as simply a "regional power"—Russia really never lost its focus on *us*. Its geo-strategic aim remained squarely targeted on the western liberal order, and more specifically, on what its KGB-trained leadership views as the "Main Enemy"—the United States.

So, Russia diligently honed and updated its toolkit for a different kind of Great Power rivalry. They couldn't match us in the old Cold War paradigm, so Russia needed a strategy that would allow them to compete with us on a new emerging battlefield. Russia's Chief of General Staff, General Valery Gerasimov, gave Putin exactly what he needed.

General Gerasimov outlined a new strategy doctrine that the Kremlin was more suited to fight, at, and then, and in this strategy doctrine, a strategy that they could win, and bring Russia back on par, as a superpower, with the West.

He recognized, and a way that I think very few within our government did, a "blurring" of the lines between war and peace, between direct conflict and indirect conflict in the 21st century. He emphasized "non-military means" and to basically advance this doctrine for "informational conflict" ... and the, and the using the measures of what he would call "concealed character." General Gerasimov outlined a vision for Russia's military doctrine that relies not just on conventional weaponry, but on a whole system of asymmetric means.

His vision of hacking, cyberattacks, information warfare, and propaganda, would be the weapons of choice. He painted a picture of the fight, of a fight really in the shadows—a type of "hybrid

warfare.” It’s a fight that I think from all the comments made by Putin *and* his allies that the Kremlin, is actually intent, not only on bringing parity, but actually intent on winning.

Now, Putin quickly put to work implementing this new doctrine. First, across the border in the Ukraine, employing the so-called “little green men,” and information warfare to create a state of perpetual chaos and instability. He also targeted Estonia and Georgia, and other countries within the former sphere of the Soviet Union. He continued to invest in this type of deniable, asymmetric tools that would help him overcome the West’s more traditional advantages. He’s now turned those weapons directly on the United States, and...I believe at *this* moment in time at least, we are inadequately prepared to take on this new challenge.

Now, in recent months, Senator Cardin and the Democrats on the Senate Foreign Relations Committee, delivered an extremely well researched report on Russia’s asymmetric assault on European democracies. They outlined a comprehensive array of weapons in the Kremlin toolkit, including the use of organized crime, corruption, energy security, and even using the Russian Orthodox Church... to increase Russia’s influence throughout the region. Now we don’t have time to get into all of those today, but I recommend everyone take a review of Senator Cardin’s valuable work.

What I *do* want to address today are the three major avenues of attack that Russia used during the 2016 campaign: first, the targeting of our election infrastructure; second, the hacking and weaponizing of information and use of those leaks; and third, the whole new realm of information warfare, particularly as it affects social media. The Senate Intelligence Committee, and again Bill I appreciate your comments, —on a bipartisan basis—is intensely focused on each of these three items.

First, truth is, that our election system has enormous strengths. The beauty and curse of our voting system in many ways is that it is fragmented and decentralized. But that thought is less comforting than it might seem when we actually step back and think how an outside power can use this decentralized system of elections in ways to attack us. We know in non-national elections that they are often decided by a few thousand votes, and while it would be difficult for any foreign power, Russia included, to attack each and every system in a national election, in a presidential year, what we need to understand is that a presidential election can actually be swung by a few thousand votes in a single jurisdiction, in a single state.

The ability for the Russians to target that to a level of specificity is remarkable. And even the *threat* of potential Russian incursion undermines our public’s confidence in our election processes. And that undermining of confidence can have devastating effects. The Russians have tremendous cyber capabilities, and we have much work to do to ensure that our **election infrastructure** can withstand anything the Russians will try. And the truth is where we stand here in the beginning of March, we are not prepared, across the nation, for the 2018 election cycle, which begins literally in a few days in terms of the primaries. We have two sets of primaries in Illinois and Texas even this month and we are not fully prepared.

Second, the Kremlin has gone to great lengths to foster one of the most permissive environments in the whole world, for malicious **cyber activity**, including both hacking and weaponizing information. While Putin maintains some of the most prolific state-sponsored cyber capabilities, much of his active measures have actually not been state-led.

The Kremlin has been able to employ and co-opt, and at times compel assistance from a detached corps of non-governmental hackers that Russia has nurtured, and harbors from international law enforcement.

Rather than always being government-led and top-down, these hackers are generally free to engage in criminal activity and money-making endeavors around the globe... as long as they keep their activities away from the private accounts of Russian oligarchs.

When it suits them, Putin and his allies are able to utilize these capabilities to further their own active measure campaigns, while allowing the Kremlin to deny involvement. Putin himself, has in many ways, trolled the U.S. by denying meddling in U.S. elections, but allowing for the possibilities of, quote, "Russian patriotic hackers" that he says: "Well I can't control *them*." Well I think there's a little more control than he's been willing to acknowledge.

Hacking is obviously not unique to the Kremlin; however, weaponizing that hacked information is a growing part of the Russian playbook.

The truth is, we should have seen this coming, even if we didn't look at all the activities that Russia had taken place in Estonia and other nations in the east, if we simply recall back in 2014, when a bugged conversation between then-Assistant Secretary of State Toria Nuland and the U.S. Ambassador to Ukraine made its way onto YouTube, where it caused a diplomatic uproar. In retrospect, we should have seen this incident as a test-run for the type of attacks and leaks that we saw during the 2016 Presidential campaign. This was an area that we should have protected better and again, frankly, we're not fully prepared for today.

Third, the Kremlin is also making unprecedented investments in 21st century **information warfare**.

During the Cold War, we all recall that the Soviets tried to spread "fake news" before that term was even popular. They assumed that the U.S. government, spread theories that the U.S. government, was involved in the assassination of Martin Luther King Jr., or that the American military had, in effect created and bred the AIDS disease. Much like today, these efforts were geared at trying to undermine basic Americans' faith in our democratic government.

But the widespread use of social media has allowed Russia to super-charge its disinformation efforts. Before, the KGB would often have to go through the process of starting setting up a newspaper in a neutral country or using a series of tools to create a dubious forgery that at its

best, whether through the newspaper, or the forgery would only hit a very small targeted group of individuals.

Now with social media, they have instantaneous access to hundreds of millions of social media accounts where propaganda and fake news can spread like wildfire. And while we all recognize the power and value of these social media platforms, if we step back and think about this from my day job on the intel committee, in many ways if an intelligence organization was trying to create a network where they could do the most damage spreading false information, and undermining people's confidence... And they could sit back and imagine what that network might look like, chances are it would look like some of the social media platforms that exist today in terms of how we gain our news and information.

The rise of these new platforms, like Facebook, Twitter, YouTube have reshaped our entire culture, and the ways we communicate and access information. But while we've marveled at the new opportunities offered by this technology, I believe our government and the technology companies themselves, have not fully understood the ramifications of these giant, new communities that they've created. And how these communities, on social media, in effect the dark underbelly, can be abused, and misused in terms of its interactions with our Americans.

Tracking the impact of Russian disinformation is obviously inherently difficult. But if we look back, to 2011, there was a Russian operations manual that suggested that disinformation "acts like an invisible radiation," silently and covertly pushing you in the direction that the Kremlin wants. Truth is, for most, you don't even know you are being attacked.

That's how Russia was able to target and co-opt unwitting Americans into spreading their content online. They even succeeded in transferring these efforts, this is one of the things that was most described in some of our hearings, from Facebook into the real world. The example we like to cite was back in the fall of 2016, where two Russian-created sites, both created out of St. Petersburg, one that catered to a more far-right group in Texas called Succeed Texas, the other which catered to a group that was about a series of the Muslim community within Texas and from a half a world away, they created an event where these two groups came into near conflict at a mosque in Houston. Think about that, the ability to manipulate Americans onto the street, and thank goodness for the police presence, or we could have had a tragedy similar to the one that took place in my state in Charlottesville, all this being manipulated and driven from a half a world away.

The truth is, this threat continues and expands.

These active measures have two things in common: First, they are effective, and second, they're cheap.

We're spending hundreds of billions of dollars on national security, and at least in this area, in terms of misinformation, and disinformation, our country is often being rocked back on our

heels. The Kremlin is spending pennies on the dollar, pennies on the dollar, and candidly wreaking havoc.

Worse yet, they haven't stopped. This threat did not go away on Election Day in 2016. Russian operatives remain active today, stoking hate and discord online.

We have seen Russian-linked accounts pushing hashtags on both sides of the NFL national anthem debate. We've seen Russian-organized hashtags and bots attack the President's National Security Advisor. We've seen them push in many ways, where it trended to the top of the list #releasethememo. And more recently, we've even seen evidence of stoking anger on both sides of the gun debate after the recent tragedy in the Parkland shooting.

And now this playbook is actually out in the open, and we have to worry about more than just Russia. These tools can be used by other actors— China, non-state actors, terrorists, and others to try to influence, and sow discord within our nation.

So...What Can We Do?

Unfortunately, there's no simple answer in this space—no single counter-measure that will stop the wave of attacks from Russia.

So, the premise of what Carnegie's Global Russia Project means, is that we have to take advantage and look at where Russia seeks to take advantage and amplify these internal divisions in our country. It's focused on boosting cynicism and tearing down Western institutions from the inside.

In response, I believe we need to start right here at home. We need to recognize the threat, expose Putin's game-plan and inoculate our society against these efforts.

In order to do that, we need to understand the Russian playbook, and deliver a thorough accounting of what they did in 2016. This is why I believe our Committee's investigation is so important. It's why I believe the Mueller inquiry, is so critical. We need to get to the bottom of what happened, and we need to do it in a bipartisan fashion. Politicization of this effort will only undermine our countrymen's understanding of the threat and truly the fact that this is not a threat against Republicans versus Democrats, but it is against a threat to our nation.

The question about whether any Americans knew about or assisted Russia's efforts in 2016 is vital. But more important, and more critical, is making sure that we make clear, that this threat did not end on election day, and that Mr. Putin's gains and aims are, is not to favor one political party over another, but is so simply sow discord and distrust within our country. And the truth is, that what we experienced, was an attack from a foreign nation.

Next, we have to recognize that we have much to do to strengthen our security and systems against these asymmetric threats. Our strategies and our resources, I believe, have not shifted

aggressively enough to address these new threats in cyberspace and in social media. The truth is if you step back and look at how we spend, Russia spends, I think the last year's budget, national-level defense-wise, was about \$68 billion. The United States of America spends ten times that much. Yet, I'd believe we're spending oftentimes on weapons that were well-suited for a 20th century conflict. We buy arms and materials to fight war on the land, in the air, and on the sea. I do not believe that we shifted near enough resources to take on, where oftentimes the 21st century conflicts will often take place in cyberspace, or in terms of misinformation and disinformation. Because until we do that, I believe the Russians are going to continue to get a lot more bang for their security buck.

No one questions America's superior technological advantages. But ironically, that technological advantage, and the technological dependence that comes with that advantage actually makes us more vulnerable in the asymmetric battlefield in terms of cyber and technology dependence that Russia has chosen to attack us in.

We must spell out a deterrence doctrine, so that our adversaries don't see cyberattacks or misinformation and disinformation attacks against us as a "free lunch." The United States, I believe, has often done too little to respond to cyberattacks against us and our allies. And when we do respond, it's often been done extraordinarily quietly, and on a one-off basis. That has clearly not been enough to deter our adversaries.

We may need to make clear to Russia and for that matter, to other nations, that if you go about using cyberwarfare or disinformation against us, we're going to call you out, and we're going to punch back.

We need to more quickly attribute cyber-attacks. We need to increase the cost of these cyberattacks against our nation. We need to use robust sanctions and other tools. And that should include the sanctions against Russia passed overwhelmingly by the Congress, but which the President has still refused to implement.

The sad truth is, that we are handicapped in our response by a lack of Presidential leadership. We need a president who recognizes this problem, and not one who sees that any discussion of Russian election interference as a personal affront. We need a president who will lead not just a whole-of-government effort, but in a sense, a whole-of-society effort, to try to take on these challenges. We need someone that will actually unify our nation against this growing, asymmetric threat.

We can't let Putin and his allies succeed. We have to—as a nation—learn how to fight back and shine a light on this shadow conflict. We have to get our act together here at home. Otherwise, we'll still be shooting blindly into the shadows.
Thank you all very much.