Sen. Mark R. Warner — "A New Doctrine for Cyberwarfare & Information Operations"
Center for New American Security
7 December 2018

Intro: Intelligence Failures

Thank you to the Center for New American Security. Thank you, Victoria Nuland and Ely Ratner for giving me this opportunity to speak about one of the most urgent challenges of our time: *the use of cyberwarfare by our adversaries…and the need to articulate a U.S. cyber doctrine.*

Today, December 7th is an auspicious date in our history. We remember Pearl Harbor as the first foreign attack on U.S. soil in modern history. Unfortunately, we also remember Pearl Harbor as a major intelligence failure.

As Vice Chairman of the Intel Committee, I've spent the better part of the last two years on an investigation connected to America's most recent intelligence failure. It was also a failure of imagination — a failure to identify Russia's broader strategy to interfere in our elections.

Our federal government and institutions were caught flat-footed in 2016, and our social media companies failed to anticipate how their platforms could be manipulated and misused by Russian operatives.
Frankly, we should have seen it coming.

Over the last two decades, adversary nations like Russia have developed a radically different conception of information security – one that spans cyber-warfare and information operations.

I fear that we have entered a new era of nation-state conflict: one in which a nation projects strength less through traditional military hardware, and more through cyber and information warfare.

For the better part of two decades, this was a domain where we thought we had superiority. The thinking was that our cyber capabilities were unmatched. Our supposed superiority allowed us to write the rules.

Blind Spots

This confidence appears to have blinded us to three important developments:

First, we are under attack, and candidly, we have been for many years. Our adversaries and their proxies are carrying out cyberattacks at every level of our society.

We've seen state-sponsored or sanctioned attacks on healthcare systems, energy infrastructure, and our financial system.

We are witnessing constant intrusions into federal networks. We're seeing regular attempts to access parts of our critical infrastructure and hold them ransom.

Last year, we saw global ransomware attacks increase by 93 percent. Denial-of-service attacks increased by 91 percent.

According to some estimates, cyberattacks and cybercrime account for up to $175 billion in economic and intellectual property loss per year in North America. Globally, that number is nearly $600 billion.

Typically, our adversaries aren't using highly sophisticated tools. They are attacking opportunistically, using phishing techniques and rattling unlocked doors.

This has all been happening under our noses. The effects have been devastating, yet the attackers have faced few, if any, consequences.

Second, in many ways, we brought this on ourselves.

We live in a society that is becoming more and more dependent on products and networks that are under constant attack. Yet the level of security we accept in commercial technology products is unacceptably low — particularly when it comes to rapidly growing Internet of Things.

This problem is only compounded by our society-wide failure to promote cyber hygiene. It is an outrage that more digital services – from email to online banking – don't come with default two-factor authentication. And it is totally unacceptable that large enterprises – including federal agencies – aren't using these available tools.

Lastly, we have failed to recognize that our adversaries are working with a totally different playbook.

Countries like Russia are increasingly merging traditional cyberattacks with information operations.

This emerging brand of hybrid cyberwarfare exploits our greatest strengths – our openness and free flow of ideas.

Unfortunately, we are just now waking up to it.

Early Warnings and Lessons Not Learned

Looking back, the signs should have been obvious.

Twenty years ago, Sergei Lavrov, then serving as Russia's UN Ambassador, advanced a draft resolution dealing with cyber and prohibiting *"particularly dangerous forms of information weapons."*

We can debate the sincerity of Russia's draft resolution, but in hindsight, the premise of this resolution is striking. Specifically, the Russians saw traditional cyberwarfare and cyberespionage as *interlinked* with information operations.

It's true that, as recently as 2016, Russia continued to use these two vectors — cyber and information operations — on separate tracks. But there is no doubt that Putin now sees the full potential of hybrid cyber operations.

By contrast, the U.S. spent two decades treating information operations and traditional information security as distinct domains. Increasingly, we treated info operations as quaint and outmoded.

Just a year after Lavrov introduced that resolution, the U.S. eliminated the United States Information Agency, relegating counter-propaganda and information operations to a lower tier of foreign policy.

In the two decades that followed, the U.S. embraced the internet revolution as inherently democratizing. We ignored the warning signs outside the bubble of Western democracies.

The naiveté of U.S. policymakers extended not just to Russia, but to China as well.

Recall when President Clinton warned China that attempts to police the internet would be like "nailing Jell-O to the wall."

In fact, China has been wildly successful at harnessing the economic benefits of the internet in the absence of political freedom.

China's doctrine of cyber sovereignty is the idea that a state has the *absolute right* to control information within its border.

This takes the form of censorship, disinformation, and social control. It also takes the form of traditional computer network exploitation.

And China has developed a powerful cyber and information affairs bureaucracy with broad authority to enforce this doctrine.

We see indications of the Chinese approach in their successful efforts to recruit Western companies to their information control efforts. Just look at Google's recent push to develop a censored version of its search engine for China.

Today, China's cyber and censorship infrastructure is the envy of authoritarian regimes around the world. China is now exporting both its technology and its cyber-sovereignty doctrine to countries like Venezuela, Ethiopia, and Pakistan.

With the export of these tools and ideas…and with countries like North Korea and Iran copying Russia's disinformation playbook, these challenges will only get worse.

And yet as a country we remain complacent.

Despite a flurry of strategy documents from the White House and DoD, the federal government is still not sufficiently organized or resourced to tackle this hybrid threat.

We have no White House cyber czar, no cyber Bureau or senior cyber coordinator at the State Department. And we still have insufficient capacity at State and DHS when it comes to cybersecurity and disinformation.

Our Global Engagement Center at the State Department is not sufficiently equipped to counter propaganda from our adversaries. And the White House has still not clarified roles and responsibilities for cyber across the U.S. government.

While some in the private sector have begun to grapple with the challenge, many more remain resistant to the changes and regulations needed.

And the American people, still not fully aware of the threat, have not internalized the lessons of the last few years. We have a long way to go on cyber hygiene and online media consumption habits.

Let me be clear – Congress does not have its act together either. We have no cyber committee. Cyber crosses numerous committee jurisdictions — frequently hindering our ability to get ahead of the problem. It's even worse in the area of misinformation/disinformation.

The dangers are only growing as new technologies such as Deepfakes — audio and video manipulation that can literally put words into someone's mouth — are commercialized.

The truth is, we are becoming ever more dependent on software. But at the same time, we are treating cybersecurity, network resiliency, and data reliability as afterthoughts.

And these vulnerabilities will only continue to grow as our so-called *real economy* becomes increasingly inseparable from the *digital economy*.

The Cyber Doctrine

If we're going to turn this around, we need not just a whole-of-government approach; we need a whole-of-society cyber doctrine.

So what would a U.S. cyber doctrine look like?

It's not enough to simply improve the security of our infrastructure, computer systems, and data. We must also deal with adversaries who are using American technologies to exploit our freedom and openness and attack our democracy.

Let me lay out five recommendations:

1. International Norms

First, we need to develop new rules and norms for the use of cyber and information operations. We also need to better enforce existing norms.

And most importantly, we need to do this on an international scale. We need to develop shared strategies with our allies that will strengthen these norms. When possible, we need to get our adversaries to buy into these norms, as well.

The truth is, our adversaries continue to believe that there won't be any consequences for their actions.

In the post-9/11 national security environment, we spent tremendous energy combatting terrorism and rogue states. But frankly, we've allowed some of our near-peer adversaries to operate with relative impunity when they attack the United States in the digital domain.

There have been some reports in the press about the U.S. supposedly punching back at second-tier adversaries on occasion.

But we've largely avoided this with Russia and China out of a fear of escalation. If a cyber-attack shuts down Moscow for 24 hours with no power, that's a problem. If someone were to shut down New York for 24 hours — that would be a global crisis.

As a result, for Russia and China, it's pretty much been open season on the United States. That has to end.

We need to have a national conversation about the defensive *and offensive* tools we are willing to use to respond to the ongoing threats we face. In short, we need to start holding our adversaries accountable.

Failing to articulate a clear set of expectations about when and where we will respond to cyber-attacks is not just bad policy, *it is downright dangerous*. We are allowing other nations to write the playbook on cyber norms.

Part of this is the result of U.S. inaction: from the late '90s into the early 2000s, the U.S. was a consistent dissenting voice in UN meetings where cyber norms were proposed. In part, this reflected our aversion to piecemeal approaches to cybersecurity. But it also reflected a view that we didn't want to be bound by lesser powers.

In 2015, there was a major effort at the UN — including the United States — to agree to principles of state behavior in cyberspace. We saw some international consensus around protecting critical infrastructure, and investigating and mitigating cybercrime.

Unfortunately, those 2015 principles at the UN failed to address economic espionage. And even the 2015 U.S.-China cyberespionage deal was insufficient.

And in 2017, disagreements between the U.S., China, and Russia at the UN led to a deadlock on the question of how international law should apply to cyber conflicts.

Little progress has been made since then.

It's true that some folks in the private sector and the NGO space have stepped up. Look at Microsoft's Digital Geneva Convention. Look at the recent Paris Call for Trust and Security in Cyberspace — signed by 57 nations, but not by the United States. This is yet another example of the U.S. stepping back on the world stage, with countries like France filling the void.

Recently, the U.S. government and the State Department, in particular, have renewed efforts to advance a norms discussion. These efforts must be elevated and strengthened.

But norms on traditional cyberattacks alone are not enough. We also need to bring information operations into the debate.

This includes building support for rules that address the internet's potential for censorship and repression. We need to present alternatives that explicitly embrace a free and open internet. And we need that responsibility to extend *not only to government*, but to the private sector as well.

We need multilateral agreements with key allies, just like we've done with international treaties on biological and chemical weapons. That discussion needs to address mutual defense commitments.

We should be linking consensus principles of state behavior in cyberspace *explicitly* with deterrence and enforcement policies.

U.S. policymakers, with allies, should pre-determine responses for potential targets, perpetrators, and severity of attack. That means clearly and publicly linking actions and counter-measures to specific provocations.

That could mean sanctions, export controls, or indictments. It could even include military action or other responses.

Now, we should be realistic about the limits of norms in shaping behavior. Let's not kid ourselves: *in the short term,* a nation like Russia that routinely ignores global norms is not going to make an about-face in the cyber domain. This should not deter us, but it should give us a more realistic set of expectations for how quickly we can expect to see results.

But the stronger we make these alliances…the more teeth we can apply to these norms…and the more countries we can recruit to them — the more effective these efforts will be at disciplining the behavior of Russia, China, and other adversaries.

2. Combating Misinformation & Disinformation

My second recommendation is: we need a society-wide effort to combat misinformation and disinformation, particularly on social media.

My eyes were really opened to this through the Intel Committee's Russia investigation.

Everyone on the Committee agrees that this linkage between cyber threats and disinformation is a serious challenge — especially on social media. In some ways, this was a whole new world for the IC.

It is now clear that foreign agents used American-made social media to spread misinformation and hijack our civil discourse.

Let's recap. The Russian playbook included:

- Cyber penetrations of our election infrastructure;
- Hacks and "weaponized" leaks;
- Amplification of divisive, pro-Kremlin messages via social media;
- Overt propaganda;
- Funding and supporting extreme candidates or parties; and
- Misinformation, disinformation and actual "fake news"

The goal was — and is — to undermine our faith in the facts…our faith in the news media…and our faith in the democratic process.

This is an *ongoing threat*, and not just to the United States. We've also seen these tools used against other Western democracies. We've seen them used to incite racial and ethnic violence in places like Myanmar.

This threat is particularly serious in countries with low media literacy. In many ways, social media IS the internet in some of these countries.

So, what do we do? How do we combat this threat?

We can start by recognizing that this is a truly global problem. A 21st century cyber and misinformation doctrine should lean into our alliances with NATO countries and other allies who share our values.

Earlier this year, Senator Rubio and I brought together a group of 12 parliamentarians from our NATO allies at the Atlantic Council. We held a summit focused on combatting Russian election interference.

Ironically, this was the very same day that our President stood onstage and kowtowed to Vladimir Putin in Helsinki. Meanwhile, we were working with our NATO allies to develop a road map for increased cooperation and information sharing to counter Russian cyber and misinformation/disinformation aggression.

In many cases, these countries are further along in educating their populations about the threat of misinformation and disinformation.

Last month, I met with the Prime Minister of Finland. As he put it, the Finns have been dealing with Russian misinformation and disinformation for over a hundred years. Finland is one of the most resilient countries when it comes to countering this threat from its neighbor to the east. Why is that?

Again, it is their whole-of-society approach. It relies on a free press that maintains trust through strong self-regulatory mechanisms and journalistic standards. It places limits on social media platforms. They also have a vibrant digital civics initiative.

Finland's approach also depends on national leadership that stays true to its values — even in the midst of contested elections and its own brand of partisan politics.

Here in the United States, it will take all of us – the private sector, the government, *including Congress*, as well as the American people – to deal with this new and evolving threat.

In terms of the private sector, the major platform companies – like Twitter and Facebook, but also Reddit, YouTube, and Tumblr – aren't doing nearly enough to prevent their platforms from becoming petri dishes for Russian disinformation and propaganda.

I don't have any interest in regulating these companies into oblivion. But as these companies have grown from dorm-room startups into media behemoths, they have not acknowledged that their power comes with great responsibility.

Recall that immediately following the election, Mr. Zuckerberg publicly ridiculed the idea that Russia had influenced the U.S. election via Facebook as a "pretty crazy idea."

Now, I don't have all the solutions. But I expect these platforms to work with us in Congress so that together we can take steps to protect the integrity of our elections and our civil discourse in the future.

Companies like Facebook and Twitter have taken some helpful voluntary steps – but we need to see much more from them. That's going to require investments in people and technology to help identify misinformation before it spreads widely.

I've put forward a white paper which lays out a number of policy proposals for addressing this:

We can start with greater transparency. For example, I think folks have the right to know if information they're receiving is coming from a human or a bot.

I've also put forward legislation called the *Honest Ads Act* that would require greater transparency and disclosure for online political ads.

Companies should also have a duty to identify inauthentic accounts — if someone says they're Mark from Alexandria but it's actually Boris in St. Petersburg, I think people have a right to know.

We also need to put in place some consequences for social media platforms that continue to propagate truly defamatory content.
I think platforms should give greater access to academics and other independent analysts studying social trends like disinformation.

We also discuss in that paper a number of other ideas in the white paper around privacy, price transparency, and data portability.

These are ideas intended to spark a discussion, and we need social media companies' input. But we're moving quickly to the point where Congress will have no choice but to act on its own.

One thing is clear: the wild west days of social media are coming to an end.

3. Harden Networks, Weapons Systems, and IOT

Third, we need to harden the security of our computer networks, weapons systems, and IoT devices.

Many of the responsibilities for cyber and misinformation/disinformation will fall on the government. But our nation's strategic response must also include greater vigilance by the private sector, which has frequently resisted efforts to improve the security of its products.

For over a decade, the U.S. thought it could set a light-touch standard for global data protection by avoiding any legislation. While regulation can have costs, what we've learned is that U.S. *inaction* can also have costs – as other jurisdictions leap ahead with *more stringent* privacy and data protections.

We see this with GDPR, where the U.S.'s failure to adopt reasonable data protection and privacy rules left the field open for much stricter European rules. These standards are now being adopted by major economies like Brazil, India, and Kenya.

More broadly, we need to think about a software liability regime that drives the market towards more secure development across the entire product lifecycle.

But nowhere is the need for private sector responsibility greater than the Internet of Things. General Ashley, Director of the DIA, has described insecure IoT and mobile devices as the "most important emerging cyber threat to our national security."

As a first step, we should use the purchasing power of the federal government to require that devices meet minimum security standards. I have legislation with Senator Cory Gardner to do this.

At least at the federal level, we need to make sure that these devices are patchable. We need to make sure they don't have hard-coded passwords that cannot be changed. We need standards to make sure they're free of known security vulnerabilities.

And on a broader level, public companies should have at least one board member who can understand and model cyber-risk.

Another area I've been working on is trying to impose some financial penalties on companies like Equifax who fail to take the necessary steps to secure their systems from cyber intrusions.

Unfortunately, even in areas where we would expect a higher level of security and cyber hygiene, we find these same problems. In October, a GAO report found that "nearly all" of our new weapon systems under development are vulnerable to attack.

Earlier this year, we successfully included language in the NDAA requiring cyber vulnerability assessments for weapons systems, which hopefully should help correct this. The Pentagon has also taken steps recently to make cybersecurity a greater priority within DoD, but frankly we face some serious workforce challenges in recruiting and retaining the top cyber professionals who have plenty of lucrative opportunities in the private sector.

4. Realign Defense Spending

This is a good segue to my **fourth recommendation**: realigning our defense spending priorities. The United States' military budget is more than $700 billion, while Russia spends roughly $70 billion a year on their military.

The U.S. is spending it mostly on conventional weapons and personnel. By contrast, Russia devotes a much greater proportion of its budget to cyber and other tools of asymmetric warfare like disinformation.

Russia has come to the realization that they can't afford to keep up with us in terms of traditional defense spending. But when it comes to cyber, misinformation, and disinformation, candidly *Russia is already a peer adversary.*

Matter of fact, if you add up everything Russia spent on election interference in 2016 and double it, that's still less than the cost of one new F-35.

I worry we may be buying the world's best 20th century military hardware without giving enough thought to the 21st century threats we face.

And it's a similar story with China.

China spends roughly $200 billion on defense, but it spends a greater proportion on cyber misinformation and disinformation. If you look at the delta between what we're spending and what China is spending on defense, they're investing more in AI, quantum computing, 5G, and other 21st century technologies. Frankly, they are outpacing us by orders of magnitude.

We need to realign our priorities while we still can. Some of DoD's budget should be redirected towards cyber defense. But we also need efforts at other agencies, including R&D funding for quantum computing and AI, as well as investments in cyber technology and cyber workforce development.

5. Presidential / Government Leadership

The **final point** is that we desperately need strong federal and Presidential leadership for any U.S. cyber doctrine to be truly effective.

Because this challenge literally touches every aspect of our society, we need Presidential leadership and a senior coordinating official to head the interagency process on this issue.

It's true, there are men and women within DoD, DHS, and other agencies who are working hard to defend the United States from cyberattacks.

But only the President can mobilize the whole-of-society strategy we need.

I do want to acknowledge some positive steps that have been taken in recent months. The White House and DoD have released two important strategic documents on cyber strategy that move us in the right direction. I also welcome the delegation of authorities to defend and deter cyberattacks below the Presidential level. This has allowed for quicker responses and greater interagency coordination.

But frankly, these efforts are inadequate.

In the most recent NDAA, Congress attempted to establish a more aggressive posture on U.S. cybersecurity policy. This includes the potential use of offensive cyber capabilities to deter and respond to cyberattacks against U.S. interests — as well as authorization to combat info operations.

It also grants the President and Defense Secretary authority to direct Cyber Command to respond and deter "an active, systematic, and ongoing campaign of attacks" carried out by Russia, China, North Korea, and Iran.

These powers, if used correctly, are important components of a cyber doctrine. But by definition they require thoughtful, decisive leadership at the top.

Conclusion

I'll leave you with some final thoughts. More broadly, we need a coherent strategy for how to deal with the hybrid approach of our adversaries.

Let me be clear about what I'm *not* saying: I am not advocating that the U.S. mimic the approach of Russia and China — the idea that states have a sovereign right to control or censor information within their borders.

Frankly, that vision is incompatible with our American values and our Constitution.

What I am saying is that we need to confront the fact that our adversaries have an approach that considers control of information an essential component of their overall strategies.

We have not only failed to recognize this situation, but over the last two decades we have tended to minimize the dangers of information operations.

The truth is, the 2016 presidential election served as a wake-up call in the use of cyberattacks and information operations.

People keep warning of a "digital Pearl Harbor" or a "digital 9/11" as if there will be a single, extraordinary event that will force us to action on these issues. But I have news for you: we are already living these events. They're happening every day.

Look at the 2017 NotPetya attack. In the U.S., we treated this as a one-day news story, but the global cost of that one attack is over $10 billion. This is the most costly and devastating cybersecurity incident in history, and most Americans have no idea.

But the true costs of our cyber vulnerabilities won't be sudden or catastrophic. They will be gradual and accumulating.

Our personal, corporate, and government data is being bled from our networks every day; our faith in institutions and our tolerance for one another is being eroded by misinformation.

This is leaving us exposed as individuals and vulnerable as a country. It's time we dramatically shift how we view these threats.

I hope the ideas I've laid out today will help us move towards the comprehensive cyber doctrine that we so desperately need in these challenging times. Thank you.

###