Sen. Mark R. Warner
German Marshall Fund – Speech
27 February 2019

Intro

Thank you to the German Marshall Fund. And thank you Ambassador Kornbluh for your kind introduction.

I am honored be here for the launch of the Digital Innovation & Democracy Initiative and to talk about one of the most pressing issues of our time: *Safeguarding against the misuse of technology*.

We can all agree that technology has completely changed the way we communicate with one another and has advanced our individual freedoms, not to mention our convenience.

But at the same time, we now see how the the misuse of technology threatens to jeopardize our democratic systems, stifle competition, deepen national security threats, and hinder workforce development.

Russia's attack on our democracy awakened a lot of people to what I've called the dark underbelly of social media — sparking overdue conversations on privacy, data transparency and other critical issues related to social media.

We also face serious threats in the cyber domain from both state and non-state actors. Not to mention the threat of misinformation and disinformation efforts by Russia and those who have copied their playbook.

More broadly, our position as a global leader on technology and cyber issues has been weakened by the retreat of the United States on the global stage — as well as by Congress' unwillingness or inability to formulate smart policy responses to the challenges we face.

I'm encouraged that governments around the world, including the EU, have begun to fill this vacuum — identifying solutions to address many of these technological challenges. But the need for U.S. leadership on pragmatic, tech-savvy policy has never been greater.

That is why I am excited and honored to be here today for the launch of the Digital Innovation and Democracy Initiative.

The German Marshall Fund has always led the way in addressing emerging threats to democracies, including notably, online disinformation.

I want to acknowledge the impressive roster of fellows taking charge of the initiative and helping shape this necessary and overdue conversation.

And I look forward to seeing you continue tackling these challenges while strengthening transatlantic ties.

Work on Intel Committee and Identifying Vulnerabilities:

As Vice Chairman of the Senate 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, <u>adversary nations like Russia have developed a radically different conception of information security – one that spans cyber-warfare and information operations</u>.

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.

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.

Just last year, we saw global ransomware attacks increase by 93 percent.

But our adversaries aren't necessarily using highly sophisticated tools – they don't need to.

They are attacking opportunistically, using phishing techniques and rattling unlocked doors.

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.

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.

China

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

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

But 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 this idea that a state has the *absolute right* to control information within its border.

This takes the form of censorship, disinformation, and social control — such as China’s social capital system. It also takes the form of traditional hacking.

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.

Working Together

As western democracies, we cannot remain complacent.

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

Congress has not had its act together either.

That's why it's important that we, as allies, work together to get ahead of the problem.

It's not enough to simply improve the security of our own infrastructure, computer systems, and data.

We must work in a coordinated way to deal with adversaries who are using technologies to exploit our freedom and openness and attack our democracy.

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 also need to develop norms with our adversaries as well.

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

Together, we 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.

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

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.

Combating Misinformation & Disinformation

Those efforts abroad should be matched with efforts here at home to make our society more resilient to cyber and information attacks. That means a society-wide effort to combat misinformation and disinformation, particularly on social media.

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

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 societies. 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. It is particularly serious when social media is the way people access the internet in these countries.

Last year, 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?

Again, it is a 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.

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.

Specifically, the major platform companies – like Twitter and Facebook, but also Reddit, YouTube, and Tumblr – aren't doing nearly enough.

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

I expect these platforms to work with governments across the globe so that, together, we can take steps to protect the integrity of our elections and our civil discourse in the future.

White Paper

Last summer, I put forward a white paper which lays out a number of policy proposals for addressing these challenges and I recognize that they intersect with many of the Initiative's focus areas. So I hope this will help get the conversation started:

We can start with greater transparency. I think folks have the right to know if the 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 they're actually Boris in St. Petersburg, I think folks have a right to know that.

We also need to put in place some consequences for social media platforms that continue to propagate truly defamatory content.

Platforms should consider granting greater access to academics and other analysts studying social trends like disinformation.
We also discuss a number of other ideas in the white paper around privacy, price transparency, and data portability

It's my hope that these companies will collaborate and be part of the solution, but one thing is clear: the wild west days of social media are coming to an end.

Harden Networks and IOT

Lastly, we need to harden the security of our computer networks and IoT devices.

Many of the responsibilities for cyber and misinformation/disinformation will fall on government.

But our strategic response must also include greater vigilance by the private sector, which has frequently resisted efforts to improve the security of its products.

I've called Congress to explore whether imposing a duty-of-care on software vendors and device-makers is appropriate.

This last week, I've asked health care stakeholders and federal agencies for input on ways to best improve cybersecurity in the health care industry. There are apparent gaps in oversight and I've been concerned about the impact of cyber-attacks.

According to the GAO, more than 113 million care records were stolen in 2015.

We need to think critically about ways to strengthen information security in this sector.

But nowhere is the need for private sector responsibility greater than the Internet of Things.

As a first step, we should require that devices meet minimum security requirements. I have legislation with Senator Cory Gardner to do this.

Vendors should also have coordinated vulnerability disclosure policies. They should have established policies for intake, handling, and remediation of bugs.

Conclusion

To conclude, the work that you all are doing is so critical.

Democracies have been at the forefront of technological innovation. In order to continue leading, we need to work together so that our policies are responsive to changing realities, while respecting individual rights and privacy.

I hope the concerns and ideas I've laid out today will help get the ball rolling on this critical conversation. And I want to thank you all for letting me be a part of this special launch.

###