it is a quarter of the size of Oregon. In my home State of Oregon, we have 4 million citizens. Bangladesh already has 160 million citizens. There is no space. That is why these camps are crowded onto hillsides and carved into the dirt, because there is no place for people to be set up on flat land where it is easy to establish facilities.

These five things are what we must do: first, for our President to be a vocal international leader and bring the international community together; second, to pass the repatriation resolution; third, to bring to the floor and to pass the sanctions bill, the Burma Human Rights and Freedom Act; fourth, to send a message to Burma and the rest of the world to invest in the education of the children; and fifth, to give strong international support to Bangladesh, which is doing all it can but is in a very difficult spot to receive so many in an overcrowded and impoverished nation.

Elie Wiesel said: ''Wherever men or women are persecuted because of their race, religion or political views, that place must—at that moment—become the center of the universe.'' Let us then make Burma and the refugee camps in Bangladesh the center of the universe and come to their assistance.

I thank the Presiding Officer.

The PRESIDING OFFICER (Mr. CASSIDY). The Senator from Rhode Island.

RUSSIAN ELECTION INTERFERENCE

Mr. REED. Mr. President, I come to the floor to continue my series of speeches about Russia's actions in the 2016 election and the threat that Russia poses for the 2018 midterm elections and our national security.

Free, fair, and open elections are the foundation of our country. The Framers created a unique system that has stood for over 200 years and served as a beacon around the world.

Regrettably, the Russian hybrid operations and malign influence against the 2016 election has put the sanctity and security of our democracy in question.

Our duty as citizens and as legislators is to recognize this crisis and take concrete steps to protect our democracy. We must foster a climate of vigilance and Federal-State cooperation when it comes to elections integrity. So today, I wanted to take a moment to review what happened and offer some steps that we should take immediately.

Some may say that there was no interference and that talking about Russia's meddling against our democratic institutions is ''fake news.'' I wish it were ''fake news'', but the facts are very clear and are acknowledged by experts of every political viewpoint. Let me take a moment to review what happened before I discuss the threat and what we should do.

Fifteen months have now passed since the intelligence community released its assessment, which concluded that the Kremlin attacked the heart of our democracy by interfering with our elections process. This operation sought to weaken our democratic institutions, amplify and exacerbate societal tensions, and generally sow chaos.

There is clear evidence that the Kremlin sought to influence the 2016 Presidential election. The key findings of the intelligence community's assessment were these:

> We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election. Russia's goals were to undermine public faith in the U.S. democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency.
>
> Moscow's influence campaign followed a Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian government agencies, state-funded media, third-party intermediaries, and paid social media users or ''trolls.''
>
> Russia's state-run propaganda machine contributed to the influence campaign by serving as a platform for Kremlin messaging to Russian and international audiences.

In February of this year, leaders of the intelligence community appeared before the Senate Intelligence Committee and reaffirmed these findings. In a related action, in February, the special counsel's office issued indictments against 13 Kremlin-linked trolls for conducting ''information warfare against the United States'' with the purpose of interfering with U.S. political and electoral processes, including the 2016 U.S. Presidential election.

These tactics are aspects of a larger coordinated operation of hybrid aggression conducted by the Kremlin, using the broad spectrum of military and nonmilitary tools at its disposal. The main tenets of the Kremlin's hybrid operations are these: information operations with cyber tools, which people commonly think of as hacking; propaganda and disinformation; manipulation of social media; and malign influence, which can be deployed through political and financial channels.

Furthermore, throughout this hybrid campaign, Russia has denied its involvement and engaged in deception to hide its fingerprints.

Russia recognizes that, for now, its military capabilities are limited relative to the United States and NATO, and it will seek to avoid a direct military conflict with the West. Instead, Russian tactics leverage their strengths and exploit our open society and free markets in ways that they hope will have a strategic impact without leading to conventional war.

As laid out in the ''Russian National Security Strategy'' in 2015, the Kremlin's approach to how they respond to conflict includes weaponizing tools and resources from across their government and society.

The Russian strategy states:

> Interrelated political, military, military-technical, diplomatic, economic, informational, and other measures are being developed and implemented in order to ensure strategic deterrence and the prevention of armed conflicts.

This strategy describes the conventional and nonconventional use of warfare as the Kremlin sees it and how Russia has utilized all the tools of statecraft to engage an adversary without, in many cases, actually firing actual shots. These different disciplines together can be called a Russian hybrid approach to confrontation below the threshold of direct armed conflict, which has been developing and escalating since the earliest days of Putin's rise to power.

Russia's attacks have not ceased since the 2016 election. As former FBI Director James Comey so presciently stated about the Russians, ''They'll be back.''

Former Director of National Intelligence James Clapper assessed that the Kremlin has ''been emboldened'' by the success of their operations to date and warned that hybrid operations ''will continue.'' At a Senate Intelligence Committee hearing in February, CIA Director Pompeo confirmed that the intelligence community has seen ''Russian activity and intentions'' to affect the 2018 midterm elections.

Director of National Intelligence Coats stated at this same hearing that our intelligence experts expect that Russia will conduct bolder and more disruptive cyber operations in the coming year. The agency heads from across our intelligence community agreed with this assessment.

The warnings from our current and former intelligence officials appear to be spot-on. There has been a steady pace of Russian hybrid operations deployed against us, our allies, and partners, with varying degrees of intensity and mixes of tools and methods. The techniques unleashed against us in the 2016 elections as laid out by our intelligence community were deployed with maximum intensity during last year's French Presidential elections. There was also evidence of hybrid operations against the German Federal elections held in September of 2017. Kremlin-linked trolls targeted the people of Spain, exacerbating divisions during the referendum on Catalonian independence. Outgoing National Security Adviser H.R. McMaster said we have seen ''initial signs'' that the Kremlin is using tools from its hybrid arsenal against the upcoming Mexican elections. After last month's poisoning of the former Russian spy and his daughter on British soil, an estimated 2,800 Kremlin-linked bots were unleashed to cast doubt on Prime Minister May's assessment that Russia was responsible and to amplify divisions among the British people. While the majority of the interference appears to have come from Russia, others are catching on and deploying these tools as well.

As highlighted in the Economist last week, a coalition of Indonesian religious extremist groups used propaganda and disinformation to affect a local election in Jakarta last year. The frontrunner, a Christian, was falsely accused of insulting Islam and huge rallies were organized against him. In the end, he lost to a candidate that

held the support of Muslim groups. This more overt interference has been coupled with covert information operations, using social media to smear candidates they deem ''not Muslim enough.''

A second Christian candidate in upcoming Indonesian regional elections has been portrayed as a front for Christian domination in a country that has an estimated 90-percent Muslim population and has been featured in a video that falsely claimed that he was part of a massive church building campaign.

With voters in this area spending an average of 4 to 5 hours a day looking at social media on their phones, videos and messages have quickly gone viral. As this example highlights, these campaigns don't even have to be sophisticated. They use tactics out of the Kremlin's playbook and they indicate how ubiquitous this type of activity is becoming across the world.

We also continue to see evidence of the Kremlin and Kremlin-linked agents deploy hybrid tools to sow division, exacerbate racial and religious divides, and amplify social tensions here at home. We don't have to look far for examples.

Kremlin-linked trolls flooded Twitter with messages intended to sow division and disinformation in the wake of the tragic shootings in Las Vegas and Parkland, FL.

During the special election to fill the Alabama Senate seat vacated by now-Attorney General Jeff Sessions, one candidate gained 1,100 Russian-origin Twitter followers over a 3-day period, with many of the accounts appearing to be artificial.

January press reports indicate that Fancy Bear—the Russian military-linked hackers who perpetrated attacks on the Democratic National Committee in the 2016 election—have been attempting to penetrate the emails of Senate offices in the run-up to the 2018 midterm elections.

Kremlin propaganda outlets RT and Sputnik continue to try to capitalize on our open press and public debates to spread disinformation and amplify division.

In sum, Kremlin and Kremlin-linked agents are still trying to hack us, our allies, and partners to fuel their information operations. They are still using trolls and bots to manipulate social media and targeting us with disinformation campaigns and still deploying propaganda.

In the absence of strategic action to deter these kinds of attacks, Russia sees our 2018 midterm elections as another prime target.

Despite this threat and multiple warnings from across our intelligence community, Trump administration officials have testified to Congress dating back to last spring that the President has not directed his Cabinet or senior staff to work on a strategy to protect our democratic institutions. When I asked Defense Secretary Mattis on June 13, 2017, whether the President had directed him to begin intensive planning to protect our electoral system against the next Russian cyber attack, he was not able to point to any guidance indicating that the President recognizes the urgency of the Russian threat or the necessity of preparing to counter it during midterm elections.

On June 21, 2017, I asked officials from the Department of Homeland Security, who are in charge of election security, whether the President had directed them to come up with a plan to protect our critical election infrastructure. They responded no.

On October 19, 2017, I asked leading officials from the Pentagon, the FBI, and the Department of Homeland Security, who are in charge of protecting critical cyber infrastructure, including our electoral infrastructure, if the President had directed them to counter the Russian threat. They could not point to any specific direction coming from the White House to do so.

On February 13, 2018, I asked the top directors of our intelligence community whether the President had directed them to take specific action to blunt or disrupt ongoing Russian influence activities. I received no affirmative responses. FBI Director Wray said he had not been ''specifically directed by the President.'' Admiral Rogers, who serves as head of both the National Security Agency and Cyber Command, responded: ''I can't say that I have been explicitly directed to 'blunt or actively stop.' '' The other witnesses could not point to any directives from the President to confront or blunt Russian influence operations either.

On February 27, 2018, I asked Admiral Rogers whether he has the authority and the capability to disrupt hacking operations where they originate. He responded that he does not have the authority from the President to go after these perpetrators and stated that the government as a whole has so far, in his words, ''opted not to engage.''

The bottom line is that the President has not directed anyone in the intelligence community, his Cabinet, or elsewhere in his administration to develop or implement a strategy to disrupt, blunt, or retaliate against Russia for its hybrid aggression against our democracy. This threat is clear, and it only grows as we move closer to our midterm elections in November. It is past time for the President to step up and provide strategic leadership against Russian interference.

Russia has gone to school on our social and political divisions and our democratic institutions and will continue to adapt. They have learned how to exploit our vulnerabilities and are planning future operations to hit our blind spots. We are fooling ourselves if we are only looking to protect against the threats from the last Russian operation. We need to be prepared to blunt what comes next.

February testimony from the Armed Services Cybersecurity Subcommittee highlights this evolving threat. Professor Richard Harknett, a cyber security expert from the University of Cincinnati, warned that Russia's 2016 campaign against our elections was the ''stone age'' relative to the sophistication of cyber activities we are likely to see in the coming elections. Similarly, Russia expert Heather Conley from the Center for Strategic and International Studies testified at the same hearing. She said:

> If we're preparing for what Russia did in 2016, it will be very different in November. It will be very different in 2020. It will look more American. It will look less Russian. And so this is adaptation. We are already fighting the last war.

As an article from the May issue of ''Atlantic'' portrayed, we may soon find ourselves in an era where doctored images are used to further aspects of hybrid operations. New technology exists that can superimpose a person onto video of an activity they did not participate in. Franklin Foer, the author, wrote of this phenomenon:

> The genre is one of the cruelest, most invasive forms of identity theft invented in the internet era. . . . A casual observer can't easily detect the hoax.

As was highlighted recently on a ''60 Minutes'' show, we know the Russians targeted election systems in 21 States in the 2016 election and that Kremlin or Kremlin-linked actors compromised websites or voter registration systems in 7 States. The fact we have not yet taken steps to correct all the vulnerabilities does not inspire confidence for the 2018 midterm elections. Former FBI agent and expert on Russian information operations, Clint Watts, said recently on ''Meet the Press,'' ''at this point we can't ensure the vote is accurate or not changed'' and that his number one priority would be protecting the elections and the vote ahead of the 2018 elections. We cannot continue to have a wait-and-see attitude with regard to the Kremlin's hybrid operations because, next time, it could and likely will be worse. They might actually be able to change ballots or tamper with voter rolls or carry out another operation entirely that we haven't even thought of.

We are behind the curve in preparing our defenses against Russian interference in 2018—these elections that are coming. Even by the administration's own admission, we are not doing enough. At an October 18, 2017, hearing, Senator SASSE asked Attorney General Sessions whether the administration had prepared to counter future interference by Russia and other foreign adversaries in the information space. Attorney General Sessions responded:

> Probably not. We're not. And the matter is so complex that for most of us, we are not able to fully grasp the technical dangers that are out there.

This is not an acceptable response to such a pressing problem. Russia attacked the heart of our democracy, and if we do not try to find solutions and guard our infrastructure, we are derelict in our duties.

One of the last acts of the Obama administration was to deem election infrastructure critical, which put it in a priority category for assistance to guard against election interference. While appropriate and important, that is the mere beginning of a solution, and we have hardly progressed in the last 14 months.

I recently asked General Curt Scaparrotti, the head of European Command, who is on the frontline of blunting Russian aggression in Europe, whether we had a sufficient whole-of-government to combat such hybrid operations. He responded that we did not have an ''effective unification'' across the government and affirmed that additional focus was needed immediately because of the nature of the threat.

We need a whole-of-government approach with the weight of the White House behind it. We need an approach that will enable coordination across the different agencies of our government and support effective outreach and collaboration with State and local officials and the private sector, including the media. Given the nature of Russia's asymmetric aggression, conducted below the level of direct military conflict, we must deploy a range of tools, including cyber; diplomacy; economic sanctions; financial investigations to counter foreign corruption, money laundering, and malign political influence; and strategic communications.

This administration has not effectively employed the nonmilitary tools in its arsenal, and it has been slow to respond in any meaningful way. The administration's dithering is exemplified in its foot-dragging in utilizing the State Department's Global Engagement Center to counter Russian propaganda and its delay in implementing sanctions to punish Russia. While recent actions to expel Russian diplomats after the poisoning of the Russian spy and his daughter on British soil and the decision to finally implement sanctions targeted against Putin's base of power are encouraging, they do not add up to a policy of effective deterrence.

In this regard, I would note that a former senior Defense Department cyber policymaker recently testified to the Armed Services Committee that a standing joint interagency task force is required to bring to bear the right capabilities and resources spread across the government to respond effectively to Russian aggression. Such a task force would utilize expertise from across our government, including the intelligence community, the Department of Defense, the State Department, the Department of Homeland Security, and the Treasury Department, and would allow effective coordination and collaboration on policy to counter Russia. The minority staff report of the Senate Foreign Relations Committee on Russian asymmetric operations in Europe recommended a similar mechanism. I think this is a good way forward, and I intend to continue to work with my colleagues on the Foreign Relations Committees and other committees of jurisdiction on how best to stand up such a capability.

The Senate Intelligence Committee, of which I am a member, has recently issued recommendations to improve election security. The committee urges retaining States' primacy in running elections and providing them with necessary assistance; creating effective deterrence; improving information sharing on threats; and securing election-related systems. All of these are important steps and should be implemented without delay.

Several of my Senate colleagues have thoughtfully incorporated these recommendations into legislation, the Secure Elections Act, and I strongly support this effort. This bill would improve information sharing between Federal Government and local election agencies, assist States with cyber security preparedness, and support them in replacing outdated and insecure electronic voting machines. I thank Senators KLOBUCHAR, LANKFORD, GRAHAM, COLLINS, and HEINRICH for their work on this bill, and I look forward to working with them on further legislation to protect the institutions that are essential to our democracy.

As I laid out, these operations against our elections are part of a broad pattern of Russian hybrid attacks against us and our allies and partners. As Vice President Biden and former Deputy Assistant Secretary of Defense Michael Carpenter reminded us in a recent article in Foreign Affairs:

> More than a decade has passed since Estonia became the first NATO country to see its government institutions and media organizations attacked by hackers based in Russia. In the intervening period, the risk of a far more debilitating attack has increased, but planning for how to defend against it has lagged.

There are countries, such as those in the Baltics, that have been dealing with these Russian threats for far longer than we have and have developed effective approaches for countering them.

Department of Defense National Guard units, which regularly deploy to Eastern Europe and the Baltics, may be uniquely positioned to share information on Russian hybrid attacks with State and local officials and explain procedures they learn from our European partners.

With regard to building credible deterrence—one of the Intelligence Committee's key recommendations—it does not appear that we have mounted an effective policy against Russia. As DNI Coats testified earlier this year, Russian influence operations in cyber space are intended to achieve ''strategic objectives'' and will continue unless and until there are clear repercussions for Russia. In February, Lieutenant General Nakasone testified to the Armed Services Committee that the Russians, amongst several other adversaries, don't fear us and have calculated that, in his words, ''not much will happen to them'' in retaliation for cyber attacks on America. Cyber Commander Admiral Rogers also testified in February to the Armed Services Committee that Vladimir Putin has concluded there is little price to pay for Russian aggression against the United States, and he has no incentive to stop these hybrid attacks. In outgoing National Security Advisor McMaster's last remarks, he even admitted ''we have failed to impose sufficient costs'' on Russia.

In the absence of Presidential leadership to set a policy to blunt Russian aggression and send the message to our foreign adversaries that we will not stand for attacks of this nature, the National Defense Authorization Act for Fiscal Year 2018 requires a comprehensive plan from the administration to counter Russian malign influence. That plan is overdue. The Act also requires that the President develop a national cyber policy, including any capabilities that be used to impose costs on adversaries in response to a cyber attack or malicious cyber activity. There is no time to waste, and I urge the administration to deliver these strategies and actually implement them, which would work toward imposing costs on our foreign adversaries.

I intend to return to speak further on these issues, as I believe the American people deserve a comprehensive explanation of the threats that face our democracy. I also intend to work with my colleagues on additional measures to secure our political system and election infrastructure against malign foreign influence.

None of this is to say that States will lose their traditional primacy over elections. Rhode Island is one of the States that is taking this issue very seriously by adopting new technologies to streamline voting and guard voter information.

My State is also working with the Department of Homeland Security to shore up election security, but election security must be a national priority, and the Federal Government must be a reliable partner. I must commend our Secretary of State, Nellie Gorbea, for her great efforts.

One thing remains clear. The Russians attacked our elections process—the heart of our democracy—and are primed to do it again unless the administration provides effective deterrence. This is not a Democratic issue or a Republican issue; it is an issue of national security. As the old saying goes, ''Fool me once, shame on you; fool me twice, shame on me.'' We have no time to waste.

I yield the floor.

The PRESIDING OFFICER. The junior Senator from Alaska.

TRIBUTE TO DIMITRI PHILEMONOF

Mr. SULLIVAN. Mr. President, today I rise, as I like to do at the end of the week, to talk about somebody in my State who has made a real big difference to Alaska and, in many ways,