Prepared Testimony and Statement for the Record of Toomas Hendrik Ilves

Bernard and Susan Liautaud Visiting Fellow ,Center for International Security and Cooperation, Freeman-Spogli Institute for International Studies

President of Estonia 2006-2016

At the Hearing on "The Modus Operandi and Toolbox of Russia and Other Autocracies for Undermining Democracies Throughout the World." Before the Senate Judiciary Subcommittee on Crime and Terrorism March 15, 2017

Undermining, subverting and overthrowing democratic governments by authoritarian regimes has a long history. In my own country, in 1924, some six years after our declaration of independence, the Soviet Union attempted a military *coup d'etat.* It failed. Sixteen years later, in 1940, another attempt succeeded, when Soviet troops stationed on the soil of the three Baltic staged simultaneous coups in all three countries, replacing the governments with Soviet marionettes, followed by fake elections in which 99 percent of the electorate voted for communist candidates.

All this would seem old hat, were it not for the blitz take-over, occupation and illegal incorporation of Crimea by Russia just three years ago. Insignia-less and masked soldiers took over the local Crimean parliament, installed a new government and two weeks later staged a "referendum" on joining Russia. 96.8 % were in favor. As far as coups d'etat go, as late as four months ago, we saw a coup attempt against Montenegro, the latest country to be invited to joun NATO. Assassinations of senior government officials were averted. Only this past Monday, British Foreign Secretary Boris Johnson blamed Russia for this latest subversion of a democracy.

Thus, in a discussion of the *modus operandi* of undermining democracies, we should focus more on *new* methods. The old ones we already know; we have seen them for at least a century.

The new weapon: IT

Sam Colt said about his Colt 45 revolver in the 19th Century that it was the great equalizer; weaker and smaller didn't matter if the smaller had his weapon. Today IT is the great equalizer. Small nations such as my own can be powerhouses in providing digital services to citizens, developing quickly and leaving large, far richer countries way behind. Unfortunately, the equalizing nature of IT holds true as well for countries and entities whose purposes and goals are nefarious.

Small groups of criminals can steal vast sums of money from far away; nations can bring down electrical grids, steal economic and other secrets… and as we have seen in Europe, alter the political landscape of democratic countries. And, as has been the case in my own country, states and criminals can form a unique for of Public-Private Partnerships.

All liberal democracies will need to rethink how to protect their electoral processes. This is especially true in Europe, the other pillar of liberal democracy in the world, where governments will face elections in the next couple of years.

If the most powerful and richest democracy in the world can have its electoral process derailed through mass disinformation, electronic break-ins and doxing (i.e. publication of hacked documents), then what awaits the elections this year in Germany, France and the Netherlands, where genuine extremist parties are rapidly gaining popularity?

The German domestic and foreign intelligence agencies already have announced that the same groups that hacked the emails of the Democratic National Committee and of Hillary Clinton's campaign chairman have successfully breached the German Parliament and the accounts of political parties and politicians. German elections take place in the fall of 2017; officials already report an upsurge in fake news.

French presidential and parliamentary elections are slated for April and June of 2017. In the Netherlands, where elections are just around the corner, Russian disinformation already played a strong role passing the referendum on the decision not to ratify the European Union association agreement with Ukraine. The heads of intelligence in Sweden and the U.K. have both warned in recent weeks about Russian meddling in the two countries' domestic politics. In Italy, with or without Russian help, fake news played a significant role defeating Matteo Renzi's reform referendum in December, leading to the prime minister's resignation.

The use of digital technology in politics has a relatively short history, although deception in warfare – and influencing a country's election outcome is warfare – goes back to the Trojan Horse of Ancient Greece. Yet the scale of deception and use of digital technology we saw in the U.S. elections is much newer.

Democracies are in uncharted territory.

Virtually every history of what is now known as "Cyber-war" or "Cyber-warfare" begins describing an attack on Estonia at six months into my presidency in 2007 when my country's governmental, banking and news media servers were hit with "distributed denial-of-service" or "DDOS attacks." Cyber attacks have a far longer history of course, but this was different. It was digital warfare, in the well-known definition of the great theoretician Carl Paul von Clausewitz as "the continuation of policy by other means."

In a DDOS attack, networks of bots or robots from hijacked computers send out massive numbers of signals to specific addresses to overload servers until they can no longer handle so many pings and they finally shut down. Without going into details, DDOS attacks are mounted by the same people using the same technology as spam, only instead of sending spam mails to massive numbers of address shotgun style, DDOS attacks target specific servers. It is underline that this activity is criminal, it is done for hire.

Such attacks had been used prior to 2007 in Estonia but primarily for extortion of net-based businesses or e-commerce. A web-based, general small or medium-sized company would find that their server was overloaded and would have to pay a criminal group for this activity to stop.

The attack on Estonia in 2007 was different and new. This was as far as we can tell the first time a nation-state had been targeted using digital means for political objectives — in our case, as punishment for moving a Soviet statue unloved by the populace. This was clearly a continuation of policy by other means. The next year, in the Russian war against Georgia in 2008, DDOS attacks were coordinated with kinetic attacks, meaning real military ordinance — a new development in hybrid warfare where targets were blinded by DDOS attacks and then proceeded to be bombed or shelled.

It is important to keep in mind, however, is that DDOS attacks do not breach the computers, they are not strictly-speaking "hacking"; they simply render servers and hence web-sites inaccessible. Which of course is enough to do plenty of damage. DDOS attacks reached a new level in October 2016, in the so-called Mirai attacks created major internet site outages in the US and Europe when the attackers used millions of IoT or Internet of Things devices to shut down the DYN domain server. Domain servers translate the name you write in when you want to access a page into the IP address of that site.

In the wake of DDOS attacks and their paralyzing impact, the focus of cyber-security shifted to more elaborate possibilities: the use of malware to shut-down critical infrastructure: electricity and communication networks, water supplies, even disrupting traffic light systems in major cities. This already does require "hacking", as we know the term – breaking into a computer system, not just blocking access. Indeed the potential danger to critical infrastructure became the primary focus of government and private sector concern, including in my own country, where we were already quite aware of cyber power.

This kind of cyber attack could mean shutting down a country, rendering it open to conventional attack. In 2010 the Stuxnet worm, which spun Iranian plutonium enriching centrifuges out of control warned us of the power of cyber to do serious damage to physical systems. Leon Panetta, Secretary of Defense from 2011 to 2013, warned in 2012 of the potential of a "Cyber-Pearl Harbor". Subsequent events such as the shutting down of a Ukrainian power plant in 2016 and again this year through cyber operations showed that such concerns were hardly unwarranted.

At the same time I should also note that one could already do considerable damage to national security and the private sector without disabling infrastructure; the hack of Sony and of the Office of Personnel Management in which the records of up to 23 million past and present Federal employees are good examples of an extremely dangerous breach that endangers a country's national security or its commerce.

All of these concerns fell into the broad rubric of symmetrical warfare. Whatever they did to you, once you figured out who "they" were, you could do back to them. Moreover, the U.S. Department of Defense has explicitly said in its cyber strategy that a cyber attack as I have described here need not be met in the cyber domain; a kinetic response is just as possible.

The rise of "Fake News": an old weapon upgraded.

False narratives have been around since the Trojan Horse, when Troy's leadership bought the Acheans narrative that they had left. Since then, false narratives have been a part of every conflict; in the Cold War, the West was under a constant barrage of fake news that, however, never really convinced anyone. Today it is different.

How and why has this changed since the fall of the Wall? For one, Western complicity: Russian fake news in the 1990s, directed almost exclusively at denigrating successful post-communist countries such as the Baltic countries and Poland, was taken more seriously by Western governments, eager to show that they took Russia seriously. I can recall numerous cases as Ambassador to the US in the first half of the 1990s as well as later in my tenure as Foreign Minister, where Western diplomats would present a false case against my country and then we had to prove it was wrong. In this case, false news was primarily an exercise in providing new democracies extra work to debunk invented news, though the propagated stories did not generally make it into the mainstream.

Following the success of Georgia during the 2008 Russian invasion in achieving narrative dominance, presenting Russian behavior as genuine aggression and not a "humanitarian action" as the Russian government maintained, Russia seems to have re-assessed and recalibrated their disinformation strategy and tactics.

By the time of the 2014 occupation and annexation of Crimea and subsequent occupation of the Donbas, Russian propaganda was heavily directed toward Western Europe, not strictly to Ukraine itself. Unfortunately Western Europe often bought the Russians' spin. Fake stories about Ukrainian "Nazis", debunked stories of atrocities were nonetheless repeated in Western media. Fake video clips (that employed the same actors playing different roles in "news stories") were used in Western television news programming. The idea that one had to "balance" genuine news with Russian "fake news" took hold and continues to the present day. News outlets and even the European Union's Foreign policy arm calls to this day Russian troops in the Donbas "Russian backed-separatists".

Given the efficacy of planting fake news in the gullible media in the West, it was hardly surprising that soon the practice was applied to Western countries themselves. Last year's "Lisa" case in Germany is probably the best known: taking advantage of Germany's growing resistance to refugees from the Syrian conflict, a confabulation by a Russian-German 13-year-old that she had been raped by "muslim-looking men" took off in the Russian and then German media. Even though the story was quickly debunked (the girl had stayed the evening with her boyfriend), Russian Foreign Minister Sergei Lavrov was still demanding an explanation from Germany two months later.

Just a month ago, within 2 days of German deployment in Lithuania as part of NATO's Enhanced Forward Presence, the Russians put out a story that *German* troops had raped a 13-year-old Lithuanian girl. The story was utterly false, yet illustrates how in the digital age fake stories can spread like wild-fire. Clearly in this media environment, the West is on the defensive.

Asymmetry in undermining democratic governments

What we have seen recently, in the U.S. and currently see ongoing in Europe, especially in countries with elections this year, is asymmetric. You can undermine a democratic election through various means I shall briefly describe, but how do you do it back to the attackers? If an authoritarian government undermines your elections, you can hardly undermine theirs if they do not have democratic elections, especially since the authoritarian government is ultimately the one to count the vote. Hacking e-mails of the rulers and publishing the more embarrassing finds does little if the media in the ruler's country are under state control and if republishing them on the web lands you in jail or worse.

In this regard liberal democracies are weaker against attacks even from relatively small cyber powers such as Iran. Similarly a small group of hackers working for a foreign government such as APT 28 and APT 29, whose exploits have been tracked in much of Europe as well as the US, can burrow into poorly protected servers anywhere. It is the *asymmetry* of such attacks that places democracies in danger: authoritarian regimes lack the vulnerability of democracies. Instead they enjoy a tactical advantage in this digital world and applying their own authoritarian mechanisms at home, are quite robust against an attack in kind..

What are the mechanisms of this asymmetric cyber war against democracies?

- Kompramat, is the Russian term for publishing (real or fake) compromising materials on opponents;

- hacking is breaking into servers and stealing data;

- doxing, combines the two: to publish hacked documents to embarrass or harm opponents. The first large scale case of this were Wikileaks' publication of some quarter million U.S diplomatic cables in 2010, the most recent only this week the publication of CIA materials.

- Finally there are fake news, an old propaganda trick but used far more effectively in the era of social media. KGB fake news in the 1980s of AIDS being invented by CIA had relatively little traction but today social media disseminates false stories with abandon.

All of these have been combined in the past year as a pincer movement on democratic elections. Hacked private mail is doxed; it appears in social and later mainstream media, after which fake news content spin on these same revelations takes off and goes "viral". Buzzfeed reported that in the last three months leading up to the U.S. election, fake news stories were shared on Facebook 8.7 million times, surpassing mainstream news by 1.4 million shares. Meanwhile, the Pew Center meanwhile reported last Summer, that for 62 percent of Americans social media was their primary news source.

Where do we stand? Democracies are in uncharted territory. Never before has private information been as vulnerable to hacking, never has it been so common to distribute it publicly and never in the past 75 years has the public been as receptive to fake news. One outcome has been a major disruption of the electoral process in several countries, which I need not go into here. Yet false stories can lead to genuine tragedy as well: after the election, a gunman with an AR-15 machine gun attacked a Washington pizza restaurant, his anger fueled by a fake story about Hillary Clinton running a child abuse ring there.

More broadly, we see the same approach is gathering steam in Europe. What we have seen in the United States and now among the European allies is that influencing a country's election outcome is warfare. Russia's Chief of the General Staff, Valery Gerassimov said as much in an article published four years ago positing that in the future hacking, cyber-warfare, disinformation, fake news etc… would all be part of one concept of warfare. He termed this "hybrid war", a concept that has received much coverage, which, however, often missed the point. Hybrid war is not about using"little green men" but rather using all tools at one's disposal to fight the adversary, and without necessarily going "kinetic".

Digital warfare as "soft power"

There is no need to wage a kinetic war or even to use debilitating cyber attacks on critical infrastructure if you can sway an election to elect a candidate or a party friendly to your interests or to defeat one you don't like. This is clearly the goal of Russia in the German elections, where Angela Merkel's role in maintaining EU sanctions against Russia has been critical and annoys Russia no end. It is true as well as in France, where Marine le Pen's Front National is anti-EU, anti-NATO and anti- US. With anti-EU and anti-NATO parties rising in popularity in a number of countries in Europe, this asymmetrical attack on the democratic process is already now a security threat to the NATO alliance.

So where to we stand?

The US intelligence services say that they the Russians were behind the Democratic National Committee and John Podesta's e-mail breaches. The Dutch are so worried about possible disruption of their upcoming elections, today on 15 March incidentally, that they are going back to paper ballots. German intelligence agencies both domestic – the *Verfassungschutz* which is their FBI – and foreign, the *Bundesnachtrichtendienst*, which is their CIA have been uncharacteristically blunt. They say outright the hacking group APT 28, run by Russian military intelligence GRU has hacked into the Bundestag as well as the servers of some political parties.

Just five weeks ago the French media reported France's Directorate-General for External Security (DGSE) believes a disinformation campaign coordinated by the Kremlin threatens to undermine April's Presidential election. They fear Russia will seek to help the anti-EU, anti-NATO National Front and its leader Marine Le Pen by using bots to massively post pro Le Pen messages online. They also fear that other candidates, most noticeably the pro-European front runner Emmanuel Macron will suffer the same hacked emails and their "doxing" or publication that cost Hillary Clinton. Russian media outlets have already begun putting out stories Macron is gay and is supported by what they call the rich gay vote. There is also a strong undercurrent of anti-semitism in the anti-macron propaganda.

British officials have said they believe Russia had a hand in the Brexit referendum and I have been told the same by Italians about the referendum called by Prime Minister Renzi on government reform last December. Certainly the number of fake news shared on social media Italy was greater than genuine referendum stories, a finding repeating the U.S. experience during your elections.

We see not only the Enlightenment values of liberal democracy under attack, but we see one of the greatest scientific creations of our lifetime, the internet turned against liberal democracy we could never have imagined when 30 years ago I worked for Radio Free Europe.

Only a few years ago we believed that the Internet, social media would be a tool of liberation, that when Middle East autocrats shut down social media, using technology to keep twitter open would allow pro-democracy protestors liberate the autocracies of the Middle East. Instead we face a dystopian landscape. These are not tools of democracy but rather are turned into tools against democracy through manipulating the electoral process. No one really thought that this can happen. Instead of helping new democracies we see our own societies under threat from fake news, by anti-democratic, often racist rhetoric that drowns out the voices of reason.

Let's not mince words. This is subversion and ultimately warfare against liberal democracies. The question remains, what is the motivation for these attacks on democracies? There is no inherent domestic of ideological reason to attack centrist governments in Europe and elsewhere. Even more perplexing should be the ideological promiscuity in supporting extremist parties: Russia supports both far right *and* far-left parties. In some cases as in Germany and Greece, both extremes of the political spectrum.

What these parties share is an antipathy toward liberal democracy and more importantly, the *institutions* that have sustained liberal democracy in Europe: NATO, the European Union, as well as of course the United State.

This puts Europe's future and the future of trans-Atlantic security in a whole different light. Europe's hitherto unity on sanctions against Russia for its behavior in Ukraine, in a foreign policy that supports democratization, difficult as it has been to maintain under current circumstances, would crumble if we see the election of a Marine Le Pen's Front National, who advocates leaving the EU and NATO and forging an alliance with Russia. Currently she is the front runner in next month's presidential election, although she is predicted to lose in the run-off that would follow a failure of any candidate to garner 50% of the vote. Similarly, Anti-EU, anti-Muslim Geert Wilders party has until the most recent poll been the front runner in the Netherlands, though there other parties have vowed to form a ruling coalition should Wilders win a plurality of votes. If predictions come to pass and Italy holds a snap election this year then the anti-EU, anti-NATO, anti-US Five Star movement is the current front runner. Like its far-right rivals, the Liga Nord, the party wants to fore close ties to Putin's Russia.

All of this seems to have one goal: to weaken the NATO alliance, to weaken the European Union and European cohesion. Against a united NATO or EU, Russia is dwarfed. Against a divided Europe of individual states, or a defunct NATO, Russia dwarfs in population and in military might, even the largest of countries across the Atlantic.

We are facing something that is clearly a policy. It is a policy of the Russian Federation to use military intelligence units to run hacking groups such as APT28 or APT29. The first one is also known as "Fancy bear", the other "Cozy Bear", both are GRU hacking units whose footprint has been found across the globe.

If we return to Clausewitz's definition of war as the continuation of policy by other means, then what we are seeing is clearly the continuation of policy by other means. And then we must think not just about critical infrastructure attacks as war but attacks on democratic elections in the same light.

To return to Russian Chief of the General Staff Valery Gerasimov's 2013 article about hybrid war – which he means as using all means at hand to achieve your ends – in turn means that in some places you use "little green men", in some places you use missiles and bombs and in some places you use doxing. All these require different responses but we need to understand that these are all part and parcel of a larger game and that in all cases we are facing a major aggressive action. Just because it is digital, electronic and people don't get killed does not mean that it is not aggression.

The conundrum that Europe will face in the coming year is whether or not to use illiberal methods to safeguard the liberal democratic state under external attack. Social media is responding, albeit slowly. Facebook has announced a system to flag fake news; Twitter and Google are looking at the issue. For some, however, this may not be enough.

In Germany, a country that for obvious historical reasons is far more attuned than most to the dangers of demagogy, populism and extremist nationalism, lawmakers have already proposed taking legal measures against fake news. Yesterday, 14 March, the Minister of Justice introduced a bill that would fine social media platforms such as Twitter and Facebook up to 50 million Euros or 53 million dollars if they do not quickly take down illegal content. This includes hate speech or defamatory fake news as well anti-semitic material. When populist, nationalist fake news threatens the liberal democratic center, other Europeans may follow suit.

Democracies stand on several key pillars: Free and fair elections, human rights, the rule of law and a free untrammeled media. Until 2016, an open media was seen as a resilient democratic pillar that supported the others. Yet, because of hacks, doxing and fake news, we can already imagine the problem all democratic societies will face in future elections: how to limit lies when they threaten democracy? How to keep parliaments and parties free of hacking? How to respond when mainstream parties or politicians *are* hacked and embarrassing e-mails is published by Wikileaks in the effort to influence the election, while parties and politicians friendly to Russia are not hacked or doxed?

In conclusion:

It is in light of this, I believe that in this age of "cyber," democracies need to think beyond the hitherto geographical bounds of security. Up until now, security was constrained by geography: NATO is the North Atlantic Treaty Organization because that's where the threats were; these threats were kinetic and by definition constrained by physical distance.

Today, unconstrained by the limits of kinetic war, by the range of missiles and bombers, by the logistics needed to support an armored division, we can succumb instead to digital aggression. In the digital age, physical distance no longer has any meaning. The range of threats we have seen in the past decade since Estonia was attacked – from DDOS attacks to wiping out communications or power grid infrastructure to disrupting elections are all independent of distance from the adversary.

Disruptions of electoral processes differ, however, because of the asymmetrical vulnerabilities of democracies to the kind of behavior we have witnessed in the past year, behaviors we now see rolled out against European democracies as well.

We in the West possess asymmetrical advantages as well; after all a Russia visa ban on supporters of Russian sanctions on such Western leaders as John McCain was met with considerable derision in the West. It is *our* asymmetrical advantage that adversaries want to vacation here, park their laundered money in safe, rule-of-law countries, buy real estate that an authoritarian leader cannot confisctae. We *can* investigate money laundering, especially in the countries favored by the adversaries, and take appropriate action. We *can* make it hard for the children of the regime to study in the West or to live here on stolen riches. In an especially piquant case Vladimir Pekhtin, the chairman of the Duma ethics committee who supported the ban of US adoptions or Russian children, sponsored a law to ban Russian's ownership abroad. Pekhtin himself meanwhile owned multi-million dollar, luxury property in Miami. His son resided in Florida

In other words, we could in the West use *our* asymmetric advantage. But we won't do that.

Which leads me to suggest that we need a new form of defense organization, a non-geographical but a strict criteria-based organization to defend democracies, countries, that genuinely are democracies...

In different contexts, both Madeleine Albright and John McCain have proposed a community or league of democracies. Neither proposal went far at the time. But the threats then were minor. Could such an organization do the job to face this new threat? I proposed already 5 years ago at an Atlantic Council event at the Munich Security Conference that we consider a cyber defense and security pact for the genuine democracies of the world. After all, Australia, Japan and Chile, all rated as free democracies by Freedom House, are just as vulnerable as NATO allies such as the United States, Germany or my own country.

It will take much hard work to create such a pact but those who would undermine our democracies are already hard at work.

Thank you