Moderator: You're listening to a podcast from the Stanford Center for International Security and Cooperation.

Michael McFaul: My name is Michael McFaul, I'm the Director here of the Freeman Spogli Institute for International Studies. Welcome everybody, a big turnout. This is a joint collaboration of various different pieces of the Center here if FSI in that our visitor, President Toomas Ilves actually intersects with a lot of different pieces that we do here with CISAC, given his interest in security and cyber security issues with the Center on Democracy, Development, and the Rule of Law, given their interest in democracy. And the Europe Institute, given the fact that you are a European and a former President of a European country.

So I see a lot of faces here today that don't normally come to the meetings together and that's really great. So I'm glad we're doing this today. By the way, if you're interested in things European, we have a double-delight for you, tomorrow at noon; we'll have Alexander Stubb who's here with us today, the former Prime Minister of Finland, a current Member of Parliament. And he'll be speaking on "Life after Trump" and "Brexit: Will Europe be able to take the Lead?" So that's tomorrow at noon. I know the event is sold-out, but if you beg with Magdalena who's somewhere here, right in the back, she might be able to get some special people in. I probably shouldn't say that, you probably can't, so never mind. I shouldn't put her on the spot, but come if you can, but please get permission first.

All right, President Ilves has been with us now for about three months or so, so he is the Inaugural Bernard and Susan Liautaud visiting Scholar here at CISAC, and with various affiliations throughout FSI. This Fellowship by the way, Visiting Fellow was designed specifically to bring people to Stanford right after they had finished a time in government. But there was another condition that they had something intellectually to contribute to Stanford University. I think we landed on the perfect first Liautaud Fellow, would be a very hard act to follow. But do send your nominations in because we'll bring in somebody next year, as well.

President Ilves has had a long interesting career, kind of the career I'd like to have frankly -

President Toomas Ilves: I read today you're going to go work pro bono for the…

Michael McFaul: Correct, I volunteered to volunteer at the Senate Intelligence Committee, they seem to be having trouble with staffers, so I'd love to intern for free. Will work for food, as people say.

He was the President of Estonia for 10 years, served two terms, prior to that he had virtually every job one could have in the Estonian government, right?

President Toomas Ilves: Except the Prime Minister.

Michael McFaul: Except the Prime Minister, okay, that's a pretty interesting job you didn't have. You know your career's not over, but he was here as Ambassador, he's served as Foreign Minister, and as we're going to talk about today, really both as a practitioner and now as a thought leader is at the intersection of technology, democracy, and security. Both when he served as President and then, thinking about these issues is broad terms. So we're going to have a bit of conversation, although it's going to be brief, from my part. We have a ton of expertise in the room just looking around so I'm going to start with a few questions. Unless you want to start with something?

President Toomas Ilves: Well, I'd like to just start - can you hear me? Okay, I'd like to start by thanking Donald Trump because Donald Trump brought the three strands of my life together. Since as a child of refugees who fled from the Soviet Union, I was always - from grade 8 I started reading the New York Times about Russia or the Soviet Union. And later on, that grew into an interest into democracy more broadly when I was a teenager, and in between I had this amazing serendipitous event in which I had a math teacher who for one semester only, taught a group of 9th graders to program, which meant that for my whole life I've been doing this more or less, one way or another.

So with the election of 2006, we see democracy which is the main thing I'm going to talk about, being under threat. Thanks to new digital technologies that have for at least the past 300 years have been electoral, liberal, democratic - well, electoral democracy, liberal democracy, have not been employed. And the finally of course at least up until now, Russia has been the country most involved in getting at democracy, though I would argue that there's no reason why other authoritarian governments cannot use exactly the same techniques that we saw _____ [00:05:32]. And as you follow the European news, is being done constantly in Europe. Just today there was another piece that the same hacking group APP28 also known as Fancy Bear, had managed to hack both the two leading German political think tanks, [German spoken], having already two years ago hacked into the entire German Parliament.

Similarly the same group has actually now been doing - setting up sites for spear phishing attacks on TV, although that had already been going on but now this has been verified. So we're in this - I think we're in the beginning of a new phase in democracy because we have these technologies that did not exist before, that are being used to undermine the way we do electoral democracy. And the responses to it, I mean there have not been too many good responses to it, but at least one worrisome tendency is that we may affect some of the other part of liberal democracy. That if we get the electoral part sort of - we want to fix the electoral part with things such as fake news and or twitter bots, that we may end up impinging on some other aspects of liberal democracy such as freedom of expression. Certainly you see movement in that direction with March 15, the Justice Minister of Germany

proposed some pretty draconian legislation on social media that does not immediately take down what is considered fake news.

So I men I think - all I can do is sort of chart the landscape for you, the answers I think will take a long time to figure out. But it is - I mean it is different from every election before, I'd say 2016, the situation we're in, you could see it before coming here and there, but then you had to be paranoid. Now, you know sometimes the paranoids in these cases the paranoids in fact are right. And I think we will have to really address this in the future in all liberal democracies and in fact, the only positive thing I can see is that maybe this might be given the asymmetry of these attacks is they can do to liberal democracies or authoritarian regimes can do it to liberal democracies, but liberal democracies can't do back to them. Because you know they count the votes so it doesn't make any difference and that may in fact cause these liberal democracies to cooperate a little more against these threats. That's like abstract.

Michael McFaul: Yes, I want to get to the typology and I want to get to the prescriptions. We have until 1:30, so we can solve this problem by 1:30, okay. But before we do so, I want to go back a little bit in history. I think when the definitive work on cyber security issues has been written, I hope it's being written right now at CISAC, it'll start with 2007. It'll start with you being attacked, I mean maybe there's - you actually know the history so inform us all about maybe there were other attacks that I don't know about. But most certainly that was a definitive moment in my understanding of these issues, and thinking about these issues. I want to hear what it was like, tell us what happened? How you responded and what you did prescriptively moving forward as a country to prevent future attacks? And how worried should Estonians still be of those kinds of attacks in the future?

President Toomas Ilves: Okay, for those of you who don't know, in 2007, April/May after the Estonian government decided to move a Soviet statue that was causing all kinds of problems; we experienced something called a D-DOS attack. It was a massive, a D-DOS attack is distributed denial of service attack in which you overload severs so they can no longer respond. That was nothing new; I mean D-DOS attacks have taken place for several years already, it was a means of extortion because you would - a small or medium sized business that did its business on the web would then be attacked, then the server wouldn't work, so they wouldn't get any business. Then they were extorted for $10,000, $20,000 if you had to pay someone.

The way these things work, is also important to know that to get a better handle on it, is that it's done by the same criminals who do spam, so when you get spam, you have these networks of bots, or robot computers which are basically your, mine, and everyone else's computer if you downloaded malware and it's secretly under the control of some other people. They would send out Viagra ads and so then, but you can reverse the operation, you can

send them towards selected servers, it's the same mechanism, it's the same people.

Now, what happened in 2007 is that it was not new, it had been done before, but this was the first sort of [foreign language] event, in which it was no longer a criminal action to gain money. But rather it was a political hack, so and why Estonia stands out is on the one hand the fact that this was all-encompassing, it hit government servers, it hit all of the newspapers, it hit the banks so effectively the country was kind of shutdown, at least the critical aspects of our functioning.

Michael McFaul: Was that scary? Did it feel like oh, my god, the Russians are here?

President Toomas Ilves: No, we didn't know it was the Russians. We had no idea. First of all, I remember how I discovered it, okay, this site doesn't work, and that site doesn't work. I called up our system admin, I said my computer - or do we have a problem. He called back and said everybody's got a problem. So that was how we figured out that this was something big, it still took a little bit of time to figure out that it was not that a cable had been severed or something. Then pretty quickly the search of the computer, the emergency response team said we are under a D-DOS attack.

Michael McFaul: Just to interrupt you because I'm interested in the details. Who did you call? Was it your IT guys?

President Toomas Ilves: Well, the first guy I called was my IT guy.

Michael McFaul: All right, it's like the rest of us, the President is calling his IT guy.

President Toomas Ilves: He answered more - it was a quicker response than you do from the Stanford IT.

Michael McFaul: So how long did it take you to figure out that it was the Russians?

President Toomas Ilves: Well, I mean first of all correlation is not causality, but there seemed to be a strong correlation between Russian rhetoric and what we saw. I mean the forensics, to figure who's done something, is fairly difficult. The expert on forensics for cyber attacks is here, Herb Glidden, I highly recommend his wonderful article in the winter issue of the - whatever it is, Journal of International Affairs. Very good article, because they always ask well, how do you know? And you see this to this day, we don't it's the Russians, we don't know it's the Koreans. Well, you have a good idea if you put all of the evidence together, but no one's going to come out in a court of law.

Anyway, so that happened, and the interesting thing which also gives you an insight into the way the Russian's work, or other people too, is that when it was all over, I want to the _____ [00:15:05] of how they saw it. And what we saw on May 9th, which was then the anniversary of - the Soviet Russian

anniversary of the end of World War II, you could see this sort of medium level of threat, some of spikes went straight up and then it continued and it dropped off. Well, why is that not a normal Gaussian curve, normal Bell curve? They said well, because the money ran out. What?

Well, it turns out that what - this is how we figured out, or I figured out how this system worked. Basically, you pay these criminal gangs or organized crime gangs that do this illegal activity, and so the attacks started - the peek attack started at 00:00:00 GMT and ended at 24:00:00 GMT. You pay by the hour or you pay by the day and then this leads to my next conclusion that given this organized crime is paid for by the Russian government or some subset of it that this gives a unique form of public/private partnership. That in Russia you don't have ISPs, Internet Service Providers, you have CSP, Criminal Service Providers.

Michael McFaul: So what was the response? What did you do to defend yourselves after that?

President Toomas Ilves: Okay, well first of all, there are a number of things. For one, since we had been already for three years, because Estonia is very developed in IT, and may have been one of the reasons why I think we were attacked. Because okay, this - we can do something to the reputation of this country that's already damaged and known as a digital pioneer. But we had been urging NATO for three years to deal with cyber issues and they kept saying ah, nah, that's not really important.

Then, when this happened, in fairly short-order NATO decided we will put a center of cyber security, a center of excellence, it's an academic institution. So that was one part of the fallout, another thing that happened which I have to commend now your colleague here, I mean when the attacks started, Condi Rice called me up and said, we're here to help. Can we do anything? By the way, the next day the President will call you; so President George Bush called me up. Again, I think it was the optics that was really important because he just said I want you to come over to Washington, you know, in four weeks. Go ahead and tell people that you've been invited by me, which again, raised the profile and you know yourself as a diplomat, that the optics often actually does even more then what the reality of the situation is.

But I mean it was a thing that focused NATO's attention much more on cyber issues…

Michael McFaul: No discussions on _____ [00:18:30].

President Toomas Ilves: No, no I mean this is an unresolved issue to this day, whether it counts, different countries within NATO have different approaches. The United States already said 40 years ago that it need not answer to a cyber attack in the same domain. Meaning cyber is a domain of warfare along with land, air, sea, and space. If you attack the United States in cyber, the United States will attack you maybe in some other way in response.

The whole issue of what is a proportional response to a cyber attack is yet to be resolved and that is one of the big conundrum that we face. Okay, if you - if you take out an electrical power plant with a missile, which you see on the radar. The missile comes and it hits it, then you know where it came from, and you probably know who did it and you know that proportional would be to take out a similar thing. Whereas, in a cyber attack even though as I said before the forensics will ultimately allow you to determine who did it, it can take a while. Because then you have to marshal all of the resources both _____ [00:19:53] and human intelligence to figure out where it came from.

Then what do you do in response to that is another thing. And so this does upset kind of the standard view of things like the terrorists and so forth. And there are two entire books which have been produced now by the NATO Center, the application of international law and warfare and also on sort of non-warfare. But two cyber attacks and it is a huge area of contention and there are protocols and conventions that can be applied and there are others that can't be. One of the big problems is that in this area, we don't have any kind of international legal framework that would apply to the people that would do these things.

Michael McFaul: Right.

President Toomas Ilves: We have one thing which was originally called the Council of Europe Convention of Cyber Crime. It was rapidly exceeded to by Japan, the United States, Mexico, and it was always countries that are not in the Council of Europe for obvious reasons. But it was a convention that obligates then those who have exceeded to extradite people to - if someone is a cyber criminal and has committed a crime, say from Estonian territory against the United States, we would then hand that person, you would say this guy did it, we would go arrest them and then we'd extradite them to the United States. This has happened a number of times, most recently with a Russian hacker in Canada.

But we've extradited some people, Latvia has extradited some people, and they're often surprised because the US sentences are rather draconian versus what European ones are. But the problem is the people who actually do this, live in countries that have not exceeded to this convention. The convention is now called the Budapest Convention, as I think I said, because now it's worldwide, but it does not have Russia, Belarus, maybe Ukraine has exceeded to it since 2014. But before that, it was another major source of both cyber crime and cyber attacks and of course the People's Republic of China. All of those countries remain outside that framework, yet being the primary sources of these kinds of criminal acts, the legal framework doesn't help us much.

Michael McFaul: So all these questions are preluded to talking about 2016, because there's a case study, I want people to understand the case study before we get to our elections. What did you do to protect your systems, your computers after this

attack? What could you do legally? Were there issues, in terms of enhancing cyber security for Estonia?

President Toomas Ilves: Well, let me tell you one thing, people say the Estonians were the first ones to be hacked; no. A D-DOS attack does not get into anything so it just stops you from accessing your bank, your newspaper and government sites. Well, we did setup some cooperation with a number of countries, we already had a little bit but it wasn't advanced enough. Because we had prepared before this incident for a potential D-DOS attack because we had our first electronic voting, digital voting.

Michael McFaul: I was going to ask you about that.

President Toomas Ilves: So one of the scenarios we thought of is that someone might attack that server and so we setup some cooperation with the Czech's and Slovenes, and a couple of other countries that we could mirror these, mirror meaning that you could still access the site even though the server in question is under attack. But we did that in a much bigger way after the attack and setup much stronger cooperation which managed to payoff for Georgia a year later when the same - more advanced form of the same kind of cyber attack took place.

Because there it was that it became hybrid, because what happened in Georgia, they would blank out an area with D-DOS attacks and then bomb it. So you would increase the _____ [00:25:03] of war because not only would you - I mean you would not know what's happening, you couldn't access anything to find out what's happening, and then you would be bombed or shelled, I don't know which one it was.

By that time, what we were doing as soon as Georgia had saw that this was happening to their sites, we then started mirroring the Georgian sites to get over this. D-DOS attacks, I would just say that - back then were done by bots of computers that had been taken over by criminal gangs, people who downloaded bad material, basically porn sites were the main source of that kind of malware. It has gotten much worse since then, in a big leap that thanks to the development of the Internet of Things, and all of these closed-circuit television cameras, refrigerators, your Amazon Echo, all of those things are so-called IOT devices.

They're machines talking to machines, the problem with these machines, at least as they are devices when they're sent out, is that they have - their passwords are usually things like one, two, three, four, five or zero, zero, zero. They're not well protected and last October, we saw a massive increase in the level of D-DOS attacks when something called the MIRAI attack in which someone first of all, some group, managed to get a huge number of IOT devices. Which were - they really are robots, it's not downloaded malware, they were hi-jacked, were increasing the number of attacks dramatically. But moreover, fixed on a genuine node, the company DYN which is a DNS company that does the - does the DN, domain name server,

one of those nodes where you type in Stanford.edu, that company changes the number into the 12 digit code that is your domain.

What happened was that there is this company in New York, it employs about 500 people, it's called DYN, you can look it up its MIRAI was the attack. Basically, by attacking this little node, it's a company that simply changes names into numbers to direct your Internet traffic. That went down and large parts of the United States and Europe were without coverage, thanks to that node being attacked. Here again, this is a step beyond for us because it's - you have far more attackers because every little machine that hasn't been properly pass-worded can be hacked. They looked at a key node that would take out a huge swath, as opposed to say focusing on my bank in Estonia which doesn't - only effects me.

Michael McFaul: I'm only on my second question, by the way, so I'm only going to go to my third one and I'll open it up. But still to Estonia before we get to 2016 here and your typology of different instruments of interference. There's the dual-sides of technology which I've heard you talk about before, and we're not spending much time on today talking about the virtues of technology and the amazing things that you have done and your country has done. The edge, I think for - it's about voting, and tell us a little bit about what you think are the virtues of the way that Estonian's vote? Tell people why they shouldn't be concerned that Estonian voters might have a greater risk of having their votes somehow manipulated because of what you've done?

President Toomas Ilves: Well, that's a whole lecture but -

Michael McFaul: I know; pretend you're on twitter.

President Toomas Ilves: It's digital voting; it's not going to an electronic machine and pushing a button. It is based on, first of all, the very strong identification system we have, which is a chip card which allows you to do two-factor authentication. And also the back end architecture which allows you only to get to your - to you, that is to your data, your little cell. And so the two things that normally people are afraid of is you can hack a password, and get in, you can only do it with - through a very high-level of security.

Michael McFaul: Higher than at Stanford you told me, right? Let's not talk about Stanford, keep going.

President Toomas Ilves: The system that Stanford uses, in Estonia we call 1.5 factor authentication because you get it over your - completely hackable cell phone. If someone really wants to get you, they can in fact eavesdrop on your cell phone so it's not that secure. I should add that Stanford shouldn't feel bad because I read two days ago, that the US Congress has ID cards with a chip, it's not really a chip. It's a sticker that looks like a chip; I'm not kidding so it looks like they're really up to date and modern, but they don't have two-factor authentication type for US government offices.

You get on and you vote; so in order to do the election, you have to get everybody individually which is rather hard, especially with two-factor authentication. Right now, for the past four elections, about 31%, 32%, 33% of the electorate votes online. Why do people do it? Well, first of all you manage to get people who are abroad. The former CEO of Skype told me about how he was sitting with his Finnish friend and Finnish and Estonia elections are always within a week of each other. And so he was like I guess I'll vote and the guy said, I have to drive down to LA if I want to vote, I won't bother.

That's how it works, to avoid some of the problems is that people can conjure up is that you can change your vote. Because as opposed to a polling place, what happens if you're voting at home and someone comes with a gun and says you will now vote for that person? Well, later you can go and change your vote and also, you can always go to the polling station and that voids your earlier vote. The interesting thing about - we have a sociology, sort of IT behavior so you study these now for six elections, initially people thought that they would urban, younger, and more left-liberal. But after three elections, it all evened out, so left, right, urban, rural, young, old it's a flat curve and has been for three elections. I think comes from the basic penetration of IT in society so that it mirrors the society pretty well.

It's one of many things that we offer in Estonia, which is part of my bigger speal saying that if you want to develop a digital society, you have to focus not on the things most governments want which is the Ministry of Financing, we can tax you better. But rather on services that people like, so voting, we have digital signature which you can do all kinds of legal documents which is a big thing. Digital prescriptions so that you don't' have to go see your doctor, at least for a refill. Most importantly, even though it's not getting much press, but in the first time ever there's been any type of operability in digital services between countries, is Estonia and Finland are going to have a mutually interoperable digital prescription. So - we get 8 million Finns coming a year and they're always having a good time and _____ [00:35:18].

Michael McFaul: The booze; the booze, the booze is cheaper.

President Toomas Ilves: I said it's much more interesting. I proposed it five years ago, but it's only now that it's coming in. But ultimately I would see all of Europe working this way that would be how the European Union should function that public services like your prescriptions, legal signatures, all these things are mutually interoperable, across borders. Unfortunately, right now Europe is the opposite which is that physical goods, people, capital, services can move across borders, but digital services with huge difficulty. And that's now with _____ [00:36:11] our Presidency is starting on July 1 and our whole thing is promoting the digital single market agenda, but that's.

Michael McFaul: So let me ask one last question and then I'll open it up to anything, by the way, this is ask me anything. Ask you about America and our elections; you arrived here right at the time that all of these issues became very germane for most Americans, who hadn't thought about them. Correlation is not causation; I think you said that earlier today. But - rip a little bit on what you've observed, what you think is going on, tell us your best-guess of what the Russian's have done, what they intended to do? And then if we have time, maybe a bit about prescriptions, but just general questions.

President Toomas Ilves: I think there are so many misconceptions about what is going on that I mean I try, do a typology of what's going on. So the term hacking an election is a useful metaphor, but it is not - does not describe anything. I mean there are numerous mechanisms, some of which I don't think anyone even understands quite yet, at least I try and don't.

But first of all, hacking is the most basic thing, going into a computer and this is what happened to the Democratic National Committee. We hear from the FBI Director that they also went into the RNC, or the Republican National Committee. The difference between the two gives rise to the next mechanism which is Doxxing, which is the term that came from the WikiLeaks, seven/eight years ago. In which you publish documents and this is where there is a difference between what happened to the Democrats and the Republicans, was that - Comey said they went into both servers, both group's servers. They only published the material from the Democratic server and so which did a huge amount of damage to the Clinton Campaign.

Already hacking into a computer like that is not something one should do, basically it is equivalent to the 1972, June break-in of the, again, the Democratic National Committee in the Watergate Hotel. The difference is that, that was physical, the people were caught which ultimately led to the resignation of the President. But the thing that amazes - that is different today, is the sociology or psychology of the media, which if you steal the physical correspondence of a political party, or as was attempted to do in 1972, there would have been universal condemnation and people would not have looked at what it is in that.

The media response and I think the New York Times even regrets it, to the theft of their purloined letters, they are stolen and then they are published. And instead of going wow, look at this; people have stolen the correspondence of a political party and being aghast at that. They - with this vulgar voyeurism, instead focused on the content of that, rather than the fact that how did this happen? Why are we even discussing this? If that doesn't help, think about having your own email hacked, and then looking for something that could be embarrassing to someone. The effect was huge; the Chairman resigned as a result, she had made some comments about Sanders. I mean who of us has not said something nasty about someone else, a third-person in our emails, which are stored on a server that may be hacked into?

So first you have hacking, then you have docs, I mean you add to that the fake news which is again, in and of itself, is nothing new. The Trojan Horse was fake news, it went away, but it didn't go away. But the provenance of fake news, of lies, thanks to this new digital environment of Facebook and twitter, the problem that we face is that it has completely changed our consumption of news. The Pew found that last June, that for 62% of Americans, the prime source of news is Facebook so I mean - it maybe the New York Times or it may be Breitbart or whatever it is but you're getting it all from Facebook.

On the other side, there's Facebook, there's Twitter where you have these - we have Twitter bots that - constantly repeat certain items so that two different followers or non-followers. The big researchers on this is the star of the Stanford baseball team -

Michael McFaul: Basketball.

President Toomas Ilves: Basketball, yeah. _____ [00:42:37] doing superb work, but I hope you invite her here sometimes. On how fake news is spread and she has a piece on media.com, from a month ago on how she started researching this when she was looking at how news of man-made disasters spread. She took as a case study, the Boston Marathon Bombing and she studied it. She discovered that all these bizarre conspiracy theories arose immediately rather, saying that Navy Seals did it. But it spread massively across the twittersphere. That's when she discovered that there are these politically motivated Twitter bots, or politically managed Twitter bots that spread conspiracy theories, or theories that things didn't happen.

These things go viral; the most recent one she looked at was the Syria, #syriahoax, which went viral, claiming that no Sarin gas or Sarin attack had occurred. And so this then becomes a trending topic on Twitter and then people who are silly enough to look at what's trending, will retweet it and it turns into an avalanche. So social media, through social media the truth becomes devalued. There's a wonderful book which I would urge even for entertainment value, to read which is by a man named Peter Pomerantsev, it's called *Nothing Is True and Everything Is Possible* about his experiences in Russia as a television producer, which is from about ten years ago. But it applies today. How he runs the entire media.

We saw sort of the explosion of fake news with the Ukrainian, in the Ukraine. Before that, there had been a lot of this disinformation being spread about - I mean within Russia, and then in Eastern Europe in terms of the Georgian war, we saw a lot of that. But when it really took off was the Ukrainian invasion, when in fact the Western media was inundated with fake news, which were then naïve enough at the beginning, picked up by Western new sources. We want a balanced picture so you have a lie about the Ukrainian's crucifying a little boy, and then the Ukrainian's saying no. And then you have the BBC saying well, we have to present both sides. They

calmed down a bit on that, when they realized there is such a thing as fake news.

All three I mentioned are new developments, now where it gets really scary to my mind, but I don't know quite the mechanism yet, is that big data analytics has gotten to the point where you - in the political process, you can basically dispense with mass communication. That - there is a company called Cambridge Analytica that does big data analytics and based on whatever you feed into it, you can pinpoint very specifically, in a very granular way your audience. And tailor your messages to them and Cambridge Analytica is a company that first was - its major investor is one of Trump's biggest supporters, Robert Mercer, along with his wife. Steve Bannon is on the Board of this company and it's CEO, give talks about how good, how well one can in fact go and send messages, target messages.

If I can find the quote somewhere here, he - the question we haven't figured out is how much of this is self-promotion and how much of it is really true. But in any case, big data analytics can in fact target audiences in a way that you know, you live on that block, your this ethnicity, you seem to be in this income range, you have a message that goes - well, here's a quote from Alexander Nix is the CEO; "A really ridiculous idea, the idea that all women should receive the same message because of their gender or all African-Americans because of their race." What they sell is targeting very specific messages, the question is you have to know who you have to target.

For me, at least, raises a suspicion of one of the other - rather unreported sides of Russia's efforts last year, which is that the voting rolls in a number of states were stolen by the Russians. The same group APP28 or Fancy Bear broke into certain state governments and stole the voting roles; now why would you do that? Because you can't really affect the vote, I mean you - you can't change their vote, but why would you want to know who's voting, if not for use in targeting specific voters.

So when you put all of this together, I mean aside from being very depressing, is that the way we do electoral democracy today - we do it the old way. But we have to understand that these - we are facing these kinds of threats to the process that we could not imagine ten years ago, or you could imagine but you have to have a pretty wild imagination. So how do we proceed? One of the things that worries me is that some of the responses at least, could in turn undermine the democratic process or liberal democracy as we know it.

Because when you see a country like Germany which really takes a very hard line on all kinds of extremism, especially right-wing extremism, having being subjected to fake news from Russia. This year, there was even a fake news story broadcast by Breitbart which said that - completely false, claiming that a thousand Muslims on New Year's Eve had burnt down Germany's oldest church. Now, when they see that and they see the reactions of the German

public, and the rise of hard-core right-wing party _____ [00:50:39] for Deutschland, they go we're not going to allow Nazi's to come back. I mean there are far more hard-core about this than anyone else, I guess they've been fairly well de-Nazified compared to some others.

So the responses may not always be so Anglo-Saxon liberal democratic as we might think because in fact, they said, the German Ministry of Justice has proposed a law that would levy up to $50 million Euro fines, $55 million dollars for any fake news that is not removed immediately. Which of course scares the hell out of companies like - well, Facebook and Twitter. But that's one possible response, at least in part of these scourges. What other things that you can do and should do is that when I mentioned two-factor authentication before, David Sanger of the New York Times said that of the 128 people with access to the servers of the DNC, 126 used two-factor authentication.

Guess who they got? Those two that did not use two-factor authentication. Not that two-factor authentication is - will give you ultimate safety but it raises the threshold for breaking in substantially. But you should use a better system then what you have here.

Michael McFaul: So that's a good place to open it up.