NATIONAL AGENDA

MIDTERM MATTERS

DAVE DEWALT

CYBERSECURITY MATTERS

HOSTED BY	University of Delaware Center for Political Communication With support from the Office of the Provost Cosponsored by the Cybersecurity Initiative, University of Delaware

PARTICIPANTS

Dr. Lindsay Hoffman	Director of National Agenda and Associate Director of the Center for Political Communication, University of Delaware
David DeWalt	Chairman of the Board for cybersecurity firm Claroty and managing director of AllegisCyber, a cybersecurity venture capital firm; former CEO of computer security company McAfee and cybersecurity company FireEye. In 2011 President Barrack Obama appointed Mr. DeWalt to the National Security Telecommunications Advisory Counsel.

Transcript of Event

Date:	September 26, 2018
Place:	Mitchell Hall, University of Delaware, Newark, DE

DR. HOFFMAN: Welcome everyone to the Eighth Annual National Agenda Speaker Series brought to you by the University of Delaware Center for Political Communication with support from the Office of the Provost. Our program tonight is also cosponsored by the Cybersecurity Initiative here at UD. I'm Dr. Lindsay Hoffman. I am the Director of the National Agenda and I'm also the Associate Director of the Center for Political Communication. This year's theme -- Midterm Matters. We'll be talking all things related to midterm elections, as well as issues that matter for the midterm elections. The CPC is a non-partisan organization and we feature speakers across the spectrum. You may recall last fall we had a conversation with Joe Biden and John Kasich. Our first speaker, just a couple of weeks ago, was Lauren Duca, an opinion columnist for Teen Vogue. She demonstrated that opinions matter and opinions can sometimes divide and offend. But, our goal here is to model civil dialogue speaking with Americans from across the political spectrum from a variety of age groups, young and old, from different backgrounds and different parts of this very diverse country. And in election years, yes, even in the midterms, it's more important than ever to talk to a variety of folks to get perspectives on issues that matter the most. Coming up we'll hear from a 16-year-old who writes a daily political newsletter with more than 50,000 subscribers; a writer from the Daily Show with Trevor Noah; and two Pulitzer Prize winning journalists from the Washington Post. And of course, the Delaware Debates will happen right here October 17th. This is also the second year of our audio essay contest with the theme Voices Matter. Check out cpc.udel.edu to find out more about that contest. If you appreciate these events, please sign up for the Center for Political Communication email list outside in the lobby and we can continue to bring you

*** Expletive Deleted

high quality programming. And you can also contribute via cpc.udel.edu/support. Yes, I'm going to be reading a lot of URL's this evening. We'll have an audience Q and A towards the end of this talk. But you can also tweet using the hashtag #udelagenda for a chance to join the discussion. Before we get started, I'd like to remind the audience that civil and courteous dialogue is vital to the success of our program. And, although it may seem that the dialogue we see is so contentious and so vicious we can come together and engage in civil dialogue. And I hope that's what we can demonstrate here. So, come open-minded and compassionate and you may come away with some real clues for open-ended constructive communication. Either way, let's all agree to be candid and courteous of other's views. So, without further ado, tonight David DeWalt is the former CEO of computer security company McAfee and cybersecurity company FireEye. He's currently Chairman of the Board for cybersecurity firm Claroty and managing director of AllegisCyber, a cybersecurity venture capital firm. He was appointed in 2011 by President Barrack Obama to the National Security Telecommunications Advisory Counsel. He has spoken numerous times at the World Economic Forum in Davos as well as panel discussions addressing world leaders. In 2015 he delivered the commencement address at UD where he graduated from, with a, a degree in computer science and engineering in 1986. So, he's a Blue Hen. At the ceremony he was also awarded an honorary Doctor of Science degree. What makes DeWalt unique is his embrace of both success and loss. He acknowledges that both of these things can make you stronger and he was a very inspiring speaker to my students earlier today. But what I hope DeWalt will talk to us about tonight, at least in part, is his career that has seen cybersecurity threats evolve from computer viruses and worms in the 1990's to advanced

*** Expletive Deleted

persistent threats to what he refers to as “attacks on subdomains of cyberspace.”

So, let’s get this conversation started.

Please join me in giving a big welcome to Blue Hen, David DeWalt.

AUDIENCE: [Applause.]

DAVID DEWALT: Hi there. She forgot to say Fighting Blue Hen, right?

AUDIENCE: [Laughter.]

DAVID DEWALT: It’s, its, just make sure I get that mascot right.

DR. HOFFMAN: Fightin’ with the --

DAVID DEWALT: Fighting Blue Hen.

DR. HOFFMAN: Yeah.

DAVID DEWALT: I always remind my parents that it’s Fighting Blue Hens, not Blue Hens, right?

DR. HOFFMAN: [Laughter.]

DAVID DEWALT: And I noticed your logo is getting a little more menacing now. The Blue Hen, right?

DR. HOFFMAN: Is it?

DAVID DEWALT: Yeah. The Marketing Department’s working on that well.

AUDIENCE: [Laughter.]

DAVID DEWALT: I enjoy that.

DR. HOFFMAN: Well, thank you so much for being here. If you could start us off just by talking about what is the current state of cybersecurity? How has it evolved since you got in, into the industry, and what can we expect from the future? A brief commentary.

DAVID DEWALT: Have we handed out cocktails yet? Have we --

AUDIENCE: [Laughter.]

*** Expletive Deleted

DAVID DEWALT: I'm going to give a pretty ominous view on things a little bit. So, I'm going to --

DR. HOFFMAN: It's going to get a little dark.

DAVID DEWALT: I'm well prepared. I'm a very positive person after all the years of being a CEO and, and a lot of optimism around the companies and building companies. But I talk about the state of cybersecurity with a, a bit of a, um, an analogy. I call it the perfect storm. And, I've talked about this for years but there's a set of conditions that are occurring in cyberspace that are essentially creating what, what I think of as a perfect storm, where all vectors of confluence are coming together to create almost a perfect environment to really affect our lives in almost every way, shape and form. So, I talk about it this way, you know, first of all, mankind over, over the centuries and thousands of years whenever they discovered a new domain we ended up having conflicts over those domains, right? So, as mankind discovers lands we would have armies, you know, fight battles over it, whether it's the oceans we'd have navies fight battles over it, the air supremacies during the wars, obviously space, and now cyberspace. And here we are basically having cyberwars and massive conflicts in this domain called cyberspace. But the conditions are so different than all the other domains like land and air and oceans and space because you can't see your enemy. You have this problem called anonymity on the internet. And because of the speed of innovation right now and capitalism we're watching such and explosion of vulnerabilities across all of our technology infrastructure. And that's just a fact. Almost every corporation is dealing with hundreds and hundreds of patches almost on a weekly basis trying to figure out how to patch vulnerabilities and all these vulnerabilities have opened up the western world and

*** Expletive Deleted

most of the world at this point to a lot of different types of attackers. So, all of these vulnerabilities have given rise to lots of attacker groups as well as attacker types and we've watched what once was just a handful of nations mostly the offensive agencies of those nations give rise to now we track well in excess of 800 adversarial groups with cyber capability. And of course, those 800 groups we track individually and they all have somewhat of a forensics kind of underpinning to them and we can track who's doing what to whom for the most part and this is the forensics of a lot of the companies that I'm focused on. But, we went from what I think of is kind of hacktivism and sensationalism as a danger as a result of all of these attacker groups, to now what I think of is, you know, high end crime, not just in our commerce systems and our financial payment systems, but now our cryptocurrency environments, now to massive espionage type activities brought on by what I call the great IP war with China. We then now are facing information warfare with Russia. And now escalating into both terrorism and warfare at a pretty unprecedented level.

DR. HOFFMAN: And IP just for those of us who don't know?

DAVID DEWALT: Oh, intellectual property. Sorry. I may; you have to fine me for every acronym I use that you don't know or --

DR. HOFFMAN: [Laughter.]

DAVID DEWALT: -- raise your hand if that's all right. I tend to use them a lot. But, think about all of these dangers. Think about all of these vulnerabilities and then it's all compounded by a couple of things. Number one is the lack of governance across the internet. And we've had a lot of balkanization to our internet substructures which has created nationalism across those internet properties which is now creating mechanisms of different governance models.

*** Expletive Deleted

Look at the United States internet model versus China's internet model, for example, versus other countries. We have really a, a complete change with the law enforcement models in cyber which is almost completely ineffective for a lot of reasons. Not a lot of law around this. We've arrested a few individuals over the years but compared to the amount of attacks and offensive results compared to the amount of arrests, let's just say we're in the point before you get to a decimal, and before you get to a digit. And, what you're finding is the success in these arenas is high, it's 99 percent oftentimes that these crimes and attacks can, can be, can be able to be perpetrated. And then of course that anonymity and ultimately, we've had a very poor defense to keep up with all the attacker groups. And one of the reasons for that is the offense in many cases is governments. So, today there's 3,152, I believe, cybersecurity companies. The market is about $120 billion in cyberspend. That's up over a 100 billion in ten years to give you an idea of how big this market has grown. But yet, most of the commercial defense is still highly ineffective to offensive governments because billions of dollars of research going into the offensive units of large superpowers compared to research and development of the largest cybersecurity company which may be in a couple of thousand engineers it's, it's a, it's a challenge and its hard to keep up. So, you have almost this perfect storm of conditions that has created the state of cyber to be super challenging and very unique in anything we've ever seen before. Couple that with we live in what we call an asymmetric theater. And what's an asymmetric theater? A, a country the size of the United States while having some of the greatest offensive capabilities probably has the greatest weakness of defense too because all of this technology has created all of these vulnerabilities which create an inability to use that offense effectively

*** Expletive Deleted

because we're so prone and so vulnerable ourselves. And that's why we've seen North Korea's attacks be so successful, Iranian attacks be so successful; criminal groups, Russian influence campaigns and others because we have such an underpinning of vulnerability ourselves and the smallest country in the world can do harm to the largest country in the world where in the physical kinetic world that probably wouldn't be the case. In the cyberspace world that is the case. Only a handful of researchers could put a tremendous amount of pain into a large country the size of the United States. So, a very interesting world we're growing up in. And in the intro, Lindsay talked a little bit about some of these subdomains and things that are going on. Some of the things that scare you is watching the social network subdomain or satellite communications, or industrial networks, or new types of areas of cyberspace that have almost no commercial defense or hygiene for security compared to what the attackers can actually do. So, we're always playing a little cat and mouse and trying to catchup. But, in a way it's a pretty, a pretty dismal environment right now and why I spend a lot of time trying to educate on this are because, and I hate to say sometimes you know you're right, but you could see some of the challenges coming to America long before they actually occurred and just because of our situation we're in. And here we are facing some of those crises sometimes now and we haven't done anything about it. So, there you go.

DR. HOFFMAN: So, yeah, no, thank you. I think it's interesting to think about this as kind of cat and mouse game. I've thought about that before. How; do you feel like the cybersecurity industry is sort of just always kind of retroactively acting to things, or do you think that we're getting to a place where they're actually responding and planning in advance?

*** Expletive Deleted

DAVID DEWALT: It's starting to get there. I think through; there's some really promising technologies that are come out; artificial intelligence has been an incredible area; data science where we can do modeling, we can look at lots of scenarios and simulations to see how the attackers may come in, and it gives us a lot more visibility to the problem than we had before. I'll give you an example. Just to tell you how hard this problem was, when I was CEO of McAfee we ended up having a, what's called a data engine which is essentially the virus engine that updates your computing device, you know, sometimes on an hourly basis or an everyday basis. We had 68 million unique signatures in that engine. This was back in 2011 just to give you an idea. So, 68 million viruses with a unique footprint or fingerprint too is what we had to stop on a daily basis and track. Can you imagine that in the physical virus world? Not so easy. And this number's only continuing to escalate. So, it's very hard in a reactive world where you see a new virus, you have to write a signature to block that virus and try to keep up with the attackers and you're always a little bit behind. Now, just in the last 18 months or so there's been a ray of hope about maybe how we can do anomalous behavioral detection using artificial intelligence tools to maybe predict a little bit more where the attackers could come in and the gap is closing a little bit in some areas. But still we're challenged in, in many places at this point. So -- should we have cocktails now?

DR. HOFFMAN: [Laughter.]

AUDIENCE: [Laughter.]

DR. HOFFMAN: Let's talk about McAfee. I think on an April 21st in 2010, walk us through what happened that day.

DAVID DEWALT: This is where my hand shakes now --

*** Expletive Deleted

DR. HOFFMAN: [Laughter.]

DAVID DEWALT: -- when you make me, remind me of that.

DR. HOFFMAN: I think this is a, a great example of not only kind of how we are in such a tenuous situation with, with cybersecurity but also for our communication student's kind of a good example of how to deal with crisis and how to, how to manage the public relations associated with a crisis. So, walk us through it.

DAVID DEWALT: Yeah. So, April 21st, 2010 is a date I'll never forget as long as I live. It was probably my, my biggest failure and then ultimately my biggest success wrapped in a single day. So, not easy to, not easy to do. But I woke up that morning at 6:00 a.m.; I get a call around 6:15 in the morning. I get a call from all our research, you better hurry in to the office; we've had a bit of a crisis. What the crisis was was we sent out a faulty release of our antivirus software essentially creating a computing environment for every computer that received our update that would prevent it from booting. And we blue-screened -- anybody hear that term -- blue-screening a Microsoft device we prevented it from rebooting and you couldn't turn the computer on. You, you could turn it off, turn it back on, it's still blue-screened because we quarantined by accident a piece of the operating system that was vital to the boot process. Now it sounds like an obvious thing you should have caught but we were racing over the night because we had an alert from one of the agencies that a particularly nasty virus was spreading and our researchers were working all night trying to come up with a remedy for that. At 6:00 a.m. we released the virus and we brought down 3.2 million computers and 1,672 companies in 16 minutes. So that wasn't a good day to show up at the office. Ha, ha.

*** Expletive Deleted

AUDIENCE: [Laughter.]

DAVID DEWALT: And literally I'll always remember these numbers because 1,672 companies got affected. Some of them were, you know, some of the most vital corporations in the world. Unfortunately, a lot were in Europe because they had woken up first and the east coast of the United States. The west coast wasn't affected too much because it was still early. But everyone trusted the security company to update the software and if we made a mistake, you know, they weren't expecting it. So, we brought down a lot of computers. Thank God after 16 minutes they realized that the release was faulty, they rolled it back and nobody else got injured. But, let's just say it took somewhere in the neighborhood of three to five days for every company to get back online because they had to literally reload the operating system that every computer, 3.2 million computers, so, that got affected. So, this wasn't as simple as just a cloud update that you might have today, let's just say. So, what we ended up doing was within an hour I created a video that maybe I'm most proud of to this day which was acknowledging it was all my fault and the company's fault and I took full responsibility for the mistake. Now, when lawyers are in your ear and communication experts are in your ear, don't, telling me not to admit it was my fault because of liability, I went against that judgement and you can see the video if you google it's under DaveDeWalt5958 which was the number of the release. But I freely admitted it was my fault and a funny thing happened, empathy. And empathy occurred because the clients realized well it wasn't a malicious attacker. They admitted it was their fault and why wasn't the other companies trying to fix the virus too? And it sort of started to spiral in a way, in a positive way. I'd already lost 40 percent of my market cap. All the television stations were in my

*** Expletive Deleted

lobby and I'm on the 11th floor thinking how do I get out of here fast and it wasn't good. But one of the companies that got injured that day was Intel Corporation. And, Intel's an amazing company. They wanted to figure out a way to never let this happen again and we designed a feature into their I Series chips using the trusted service memory layer to enable us to reboot automatically in the event of a catastrophic failure to the operating system and a few months later, less than 90 days later they bought the company for almost 8 billion dollars in cash which was a positive outcome in which not only did we recover the stock value, we went up another 60 percent in value. Not one company sued us. In fact, we did more business with those 1,672 companies in the next three-month period than they had done in a lifetime with McAfee. So, wow, is that a communication story. At least how I learned. And I always tell the story, like, about honesty and humility. And, whatever was natural or the way I grew up, it was just one of those moments where I felt like honesty and humility was just super required because of what had occurred and I had to admit the mistake that occurred. Thank God I did it so quickly and got out in front of the news cycle and the companies rallied behind me and rallied behind the company and we ended up getting elevated. And then Intel bought the company and that was a good outcome for our shareholders and our employees and a pretty amazing story. But, kind of a crazy day.

AUDIENCE: [Laughter.]

DAVID DEWALT: Not one I recommend waking up to regularly.

DR. HOFFMAN: Well, at, at the risk of a This is Your Life moment, I believe we actually do have that video --

DAVID DEWALT: Oh, you have the video.

*** Expletive Deleted

DR. HOFFMAN: -- pulled up.

DAVID DEWALT: Oh, God.

DR. HOFFMAN: [Laughter.]

AUDIENCE: [Laughter.]

DR. HOFFMAN: Would we like to go ahead and play that --

DAVID DEWALT: Oh God, you found it --

DR. HOFFMAN: -- for everybody?

DAVID DEWALT: -- online.

AUDIENCE: [Laughter.]

VIDEO: [Video plays.] Hello, my name is Dave DeWalt and I'm the President and CEO of McAfee. Last Wednesday, April 21st McAfee responded to a new global threat to Windows PCs and released --

DAVID DEWALT: I look younger.

VIDEO: -- a virus signature file that caused some of our customers computers to shutdown until they could be repaired and rebooted. I take full responsibility for what has occurred, and I want to take this opportunity to offer you my deepest apologies on behalf of McAfee and underscore how extremely sorry we are. Even among the vast majority of customers who did not experience operating disruptions the mere possibility created an unwelcome distraction and reason for concern. We've been --

DR. HOFFMAN: Oh, that's --

DAVID DEWALT: All right, you can cut it from there. Yeah.

DR. HOFFMAN: [Laughter.]

AUDIENCE: [Laughter.]

DAVID DEWALT: You get the idea.

*** Expletive Deleted

DR. HOFFMAN: Maybe that's good enough. You guys can watch it later.

DAVID DEWALT: You know the biggest mistake I made in that video -- I don't know if you caught it -- which is in hindsight in communications I made one error. Does anybody know what the error was? It's probably the biggest single error I made in that video and it was already said. I said the vast majority of customers who didn't get affected, you know, we were, we were concerned with but what happened to the one percent that did? So, they all felt even more terrible because they weren't in the vast majority that did. So, I shouldn't have overstated the vast majority did not get affected and those who were affected felt even worse by that one statement. Now, in the grand scheme of what we went through and how we helped them later, you know, was a positive outcome. But I learned in communications, never minimalize numbers, minimize numbers when you don't have the context for everybody else. So, that was a little bit of a learned lesson there because everybody was like wait, I'm in the one percent; why am I in the one percent? And the CEO's were asking their chief security officers why was the vast majority not affected but we were?

DR. HOFFMAN: Um-hum.

DAVID DEWALT: And, so that kind of snowballed a little bit. And, in my learned lesson of communications in a crisis is, you know, numbers matter; timing matters and in that case, I shouldn't have probably said vast majority didn't get affected. So, anyway --

DR. HOFFMAN: Yeah --

DAVID DEWALT: -- things you learn, right --

DR. HOFFMAN: --so -- yeah, so --

DAVID DEWALT: -- under duress.

*** Expletive Deleted

DR. HOFFMAN: -- a couple of weeks ago we learned opinions matter, people who have opinions it seems important for them to express them. It's also important to understand timing and strategy in communication and how you communicate that effectively. So, I think that's a great example. I'm going to switch things a little, up a little bit because, um, most of our students are very engaged in social media. We've talked about this a lot today –

DAVID DEWALT: Really? Is that true?

AUDIENCE: [Laughter.]

DR. HOFFMAN: Yes. There's like this Facebook and Twitter and Snapchat and we just saw today that there were some social media companies and large tech companies on the Hill today talking about issues related to privacy but Mark Zuckerberg sat in front of the Capitol, sat in Capitol Hill answering what, this is a question from a student Natalie (phonetic sp.) in our class, answering what the Daily referred to as what seemed like a really bad tech support call. [Laughter.] Um, if you had been in the position where Mark Zuckerberg was in when he was kind of having to answer for some of the trouble that happened in the 2016 election would you have done it differently?

DAVID DEWALT: I guess the first thing I'd say is I'm appreciative that he's there. And, for whatever it is worth there is a lot of challenges that went on at Facebook during that election process and, and issues but owning it later at least he's doing, and I applaud that, right? So, in a lot of ways trying to fix it now. He doesn't have to go in front of some of those, some meetings he, he, in a lot of cases he's testifying voluntarily to try to improve. So, I, I, I'd just start with that because a lot of companies will hide in a crisis, not, you know, step forward. You know, I always talk about bats and moths in a crisis. You know, bats and moths,

*** Expletive Deleted

some step forward into the light like a moth and some step back in the light and you know, which one are you? And in that case, I was happy to see a step forward and I thought that was to be applauded. But –

DR. HOFFMAN: But, then don't you get zapped? [Laughter.]

DAVID DEWALT: [Laughter.]

AUDIENCE: [Laughter.]

DAVID DEWALT: Don't fly too close to the light, that's the key.

DR. HOFFMAN: [Laughter.]

AUDIENCE: [Laughter.]

DAVID DEWALT: You know, just have it, just have it right. But, you know, listen, there, there's a lot happening obviously in the election process and I think for Facebook and it comes down in cybersecurity a lot of times to visibility. Do you have visibility to what's happening in your platform? Unfortunately, Facebook did not have a lot of visibility to what was happening in the platform. Nobody really did. And unfortunately, who was to see the, you know, thousands and thousands, tens of thousands of ads, tens of thousands of false identities that were being set up, the social influence campaigns, the automated software that was distributing that content. That was not easy to see when you have a billion users on your platform. And it was hard to see they were in precincts in, in battleground states and how the influence was occurring and what divisive content was created. So, hindsight is 20 – 20. But, you know, having said that, I mean, it occurred. We had a, a major, a major effect on our democratic processes and, you know, curious, I'm sure we'll talk about a little bit is like what are we doing to prepare for it. But, the fact that they're there, they're working hard on it is highly encouraging, so.

*** Expletive Deleted

DR. HOFFMAN: Well, and, to follow-up on that, when he appeared before Congress several senators actually revealed that they didn't know very much about Facebook. Orrin Hatch actually asked, so how do you sustain a business model in which users don't pay for your service? Is the disconnect between what's happening in government and what's happening in the tech industry ultimately damaging to how secure we all are?

DAVID DEWALT: Yeah, you really find that and I, I have discovered this even, you know, I'm, I'm in my 50's now but you realize the technology gap I have even to the students that are here, but you really see it to our congressmen and women and senators with their age demographics and that's no, that's no knock on them. But, they didn't grow up necessarily in the, in the knowledge era and computing eras that others did, and you can really see it just like: how do you make money on a, on Facebook? Right? Or, you know, what, what's there if they don't pay for it? Like, these are really commonsense things perhaps to us but if you didn't grow up in that era you don't know. And then you also don't know what –

DR. HOFFMAN: Well, and so let's explain how do they make their money?

DAVID DEWALT: Well, just through advertising, impressions and obviously, you know, a lot of content that is being distributed on a paid basis. Obviously, this is an era that, you know, new consumer models are being created. I mean, right now there's 3.8 billion users on social media platforms. There're 83 social networks, considered social networks, 83 of them with over 100 million users active. So, if you think about that. Now, there's overlap across those 83 networks, but, I mean, we've never seen anything like this. This all showed up in the last couple of years and the content virality is off the chart. So, we had a

*** Expletive Deleted

crisis, Lindsay didn't mention, I, I chair Safety and Security for Delta Airlines. Proud to be on the Board. And, when there's a crisis with the airline, whether it's something that seems small like a passenger, you know, perceived to being booted off the flight for some disruptive -- we could get a hundred million views in an hour. And, we're living in an era of speed of information and perception that the information I'm seeing is true therefore you're guilty before you could even reply. And so, this type of network and this type of information is something brand new to this world in a way that we don't know how to interact with. And frankly, even the founders of these companies are still wrestling with how big their platforms have become, how important their platforms are, how influential those platforms are, and what do we do about it? I, I talk a little bit about what I call the 55 states of America. Some of the students heard this. But, the 55 states of America not only the 50 states that you know but the 5 technology companies that are bigger than any individual state has become, and these being Apple and Amazon and Microsoft and Facebook and Google; two of which have crossed a trillion dollar market cap this past year; many of which are having cash flows bigger than any single state, bigger profitability, almost immune to regulation, global companies. And, if Apple decides not to let your phone get open for privacy reasons even though there's a terroristic threat to that device, so be it. Tim Cook decides. No knock on Tim but it's the reality of what we're dealing with. We now have five corporations that are so powerful and so massive and we're so reliant on their technology for what we see, what search results we see, what influence we might get on that social platform. Do we trust their integrity, their ideology? It's a real question. And who governs them for what search results you see. They're testifying about that now. But ultimately

*** Expletive Deleted

what algorithms go into that – it's a fascinating situation that we're in. And, there's almost no end in sight because the distance of the 50 states and the GDP versus these corporations are only getting wider and wider. And they're not beholding to an individual country necessarily. They do operations all over the world. So, we have a fascinating challenge coming with these technology companies' power. And ultimately their responsibility of that power is really going to fall on probably their consciousness as opposed to law.

DR. HOFFMAN: Hum.

DAVID DEWALT: Or, to national, national interests because they are so global and you're finding that a, a very new situation, in my opinion, that we've never seen before. And, it's a little tongue and cheek saying 55 states because there's a few other corporations rising amazingly too. And, the five largest companies, you know, five of the largest companies now don't even make a single product. You think about Air, Airbnb and Uber, you know, these companies. The eBay's of the world, they don't even make a product, you know, they're just brokers for other people's technology. And ultimately you have a, a really fascinating situation coming in the next few years with power struggle between government and corporation.

DR. HOFFMAN: Well, it's interesting you bring up this kind of consciousness that has to guide what, what these big five, or, you know, the, the extra five states are doing. A lot of my students have been really interested in following the controversy around Alex Jones of, of Infowars. And Katherine (phonetic sp.) a student in National Agenda asked, in August many social media platforms including Apple, Facebook, YouTube, Pinterest, and Spotify banned Alex Jones for violating their policies but Twitter didn't initially ban him saying that he didn't

*** Expletive Deleted

break any of their policies. Do you think social media platforms have a responsibility to remove high profile users who use the platform to spread conspiracy theories and or hate speech?

DAVID DEWALT: So, you've got to think about this for a number of angles. So, you can ask me, Dave DeWalt, my opinion as a consumer and citizen of the United States and I would say I do, they do have a responsibility to govern what's right and what's wrong. I think that's just humankind to, to do what's right and wrong. That's my view. If I'm an investor now and I'm a shareholder in these corporations or I'm a board of director I have fiduciary responsibility, duty of care as it's called, to essentially manage the shareholder value of that corporation which may be in conflict to the ideology of doing right and wrong necessarily about that. So, that gets very interesting as well. There is no components of our duty of care necessarily in our board governance models and shareholder governance models that is talking about these types of topics now. And so, it's all new ground again I think we're getting into in the world of cyberspace and influence in that space that we haven't covered. Very little code of conduct type policies are even in place in large corporations. It's, it's creeping in a little bit more and every country has slightly different views on that. So, again it's, you know, very new territory for the world to see how do we interact with sort of the question of right and wrong and is it right or wrong from which nation's viewpoint is, is very interesting, you know?

DR. HOFFMAN: Well, I think, we can't really talk about cybersecurity issues without talking about 2016. The presidential election and Russian meddling is the word we keep hearing. So, we; it's widely acknowledged that Russia did have something to do with 2016, but how strong is the evidence of election

*** Expletive Deleted

meddling? This is a question from my student Noah (phonetic spelling). And, something we talked about earlier, earlier today is the Mueller investigation. Do you think that there's evidence of collusion?

DAVID DEWALT: My, you asked a lot there, huh? Um. I'll answer it this way. I'll, I'll just tell you, so almost 20 years in cybersecurity I had two large epiphanies in my career. Like just major epiphanies like wow, pinch me, is this happening kind of moment. And, one of them was at the end of 2008. I told the story of now the company name that I have NightDragon Security but ultimately, I was privy to a major campaign the Chinese Ministry of State Security essentially imposed on high tech corporations in Silicon Valley, made famous by Google who ultimately pulled out of China as a result of seeing evidence of Chinese infiltration and exfiltration of source code and bug research out of Google. Pulled out of China; blamed China. We sold out 153 times that day, and, or that, that period, and we realized China and its military was attacking commercial companies on American soil. That was a bit of a like a wow moment because government on government espionage, okay, we can live with some of that activity. I was seeing a lot of that. But the first time a giant super power was inflicting a campaign on leveling the playing field of innovation between the United States and China. And as a result, during my days as CEO of FireEye and Mandiant we ended up responding to 5,772 -- and I'll repeat that -- 5,772 confirmed Chinese espionage breaches on American companies. That is a stunning revelation and epiphany to me and over a seven to eight-year period we did very little about that. China was able to level the playing field quite a bit. I called it the great IP war, intellectual property war as I said. But the second epiphany happened exactly what you said, Lindsay, was really that election

*** Expletive Deleted

window was a period of time where I realized Russia had declared a similar warfare tactic on America in a very brazen way that China did. And, if you go back and look at some of the reports that we published for China we called them the "Comment Crew". They weren't hiding. China didn't even hide. They put comments in Mandarin some of which, sorry if I swear here, would say *** you, America in the comments. And, you know, would literally call out America as part of their campaigns to level the playing field. So, we knew it was China. We tracked them to their keyboards in Beijing. We called them 61398. It was the unit that was -- like we had them. Like we, we knew it. And the same certainty of epiphany I have with Russia with what I saw. And, ultimately, we made quite arrests so what's the evidence? We arrested 18 people as part of the internet raiding agency, a Russian shell that was set up. They set up automated software. They would set up false identities, tens of thousands of false identities. They would use those false identities which would look like Americans just like you. They would put them in precincts in, in battleground states. They would create friends and followers around that social media and they'd send divisive content everyday automated from the letter A to Z in name putting out that content, changing the sentiment of Americans cultural kind of challenges. And it would be a Black Lives Matter here or it would be a anti-Hillary message here, or a religious message here, or a racism message there. And we were watching that content come out. Now, this was a little bit in hindsight because once we did the report we ended up seeing all of that, but we couldn't see it at the time. Neither did Facebook. But the epiphany that the Russian GRU had implemented this was 100 percent, in my opinion. It's not just my opinion, it's everybody's opinion. It's in the world of cyber. We ended up arresting people and shut down

*** Expletive Deleted

agencies as a result, or companies that were operating in this way and, you know, how big was the sentiment change? I don't know that. Did it look like it was in the millions and millions and millions of people? It sure did to me because you could track it by sentiment. You know, what were they liking, what were they following, what did they open, and more and more they were opening an anti-democratic, anti-Clinton message. So that brought out a lot of voters from what I could see that either didn't vote for Hillary or voted for Trump and it looked like that was a massive change in the model that occurred. We do know this, there was no affect we believe to the actual people voting -- 59 million people voted for Trump, 62 million people voted for Hillary, I think were the numbers and those were actual counts -- but the change during that period. One other piece of data, we were hired on several cases to monitor the night of election servers and things and ultimately, we stopped seeing intrusions into those servers or probes into those servers and we wondered why. It was like crickets. It was suddenly like why isn't; why aren't we seeing this because we thought that we would see that just from all the reconnaissance we had, and it stops. And we didn't see anything through election night. Which we went, wow that's great; nothing happened. But then in hindsight we saw the social influence was working, that's why they stopped going through the front door; they went through the side door of social influence that ultimately was the way in which they undermined our processes.

DR. HOFFMAN: So, they were relying on other people to share, continue sharing that information?

DAVID DEWALT: False identities.

DR. HOFFMAN: Um-hum.

*** Expletive Deleted

DAVID DEWALT: Right. So, they would set up, I think one of them was Susan Atkins, I forget her name. But they would start with the letter A; they'd set up an identity, look like an American, put that American into a Ohio in a (sic) area of Ohio, create friends and followers all around that person and start, Susan would start sending information out to all of her neighbors. And then the neighbors would start to share that information all of which had content integrity issues, but it wasn't even true. And so, you would start to see, you know, the influence campaign working. And, if you're a Russian intelligence agency and you're actually seeing people read it, open it, share it, say like to it, well, let's do more of that. And, the machine was cranking by the election process and the night of the election. Particularly during the Comey period right before the election, we saw a massive amount of that going on. So, you can decide, you know, Americans still voted. Americans got influenced, yes or no. But, certainly the facts of what occurred seem obvious to me.

DR. HOFFMAN: Where are those cocktails?

DAVID DEWALT: [Laughter.]

AUDIENCE: [Laughter.]

DR. HOFFMAN: [Laughter.] It's a little scary, right? Well, so, well the midterms are approaching, and I think a lot of our students and community members have questions about is the intelligence community prepared for whether Russia is still trying to interfere in U.S. politics; what has changed about how they're dealing with the threats since 2016; what should they be doing in the midterms of 2018?

DAVID DEWALT: And this is where we have one of our biggest challenges. I, I talk about the privacy pendulum with the security pendulum. As the privacy

*** Expletive Deleted

pendulum swings to the privacy side the security becomes weaker and when the security becomes stronger and the pendulum slides there privacy becomes more of a challenge. And, so right now the pendulum of privacy swung a little hard with what's called GDPR and some of the regulatory components coming out of Europe that American companies have to follow. And of course, post-Snowden and some of the FISA warrants that were limited and the ability for agencies to interact with corporations in a way to have them help with that social influence problem has waned to less security and more privacy. So, you know, we're aware of the problem, the question is how much influence is still occurring. You're certainly seeing Facebook and others do a lot more effort to shutdown false identities. We're reading about that constantly. We're seeing that constantly. There's more software now that helps look for anomalous behavior than we've ever had before, certainly in 2016. So, you know, we've upped our game but technology's up too –

DR. HOFFMAN: Um-hum.

DAVID DEWALT: -- so we'll, we'll see as we figure out what the affects were.

DR. HOFFMAN: One thing I think that's interesting is there's been some polling recently on how Americans feel about the upcoming midterms and how concerned they are about whether their vote will count and whether they are; whether the, the, the midterm elections will be valid. And so, this is a poll from NPR and Marist who said that, actually demonstrated there's a large partisan gap, which interests me, in perceptions that the U.S. is prepared to keep the Fall midterm elections safe and secure. So, a majority of democrats say the U.S. is not prepared and under 20 percent of republicans say so. So, first of all do you, kind of expanding on that, do you think the U.S. is prepared, and second, why is

*** Expletive Deleted

there such a large partisan gap between democrats and, and republicans -- if you can speak to it -- in terms of how we're prepared or not? Is it simply because we're in a republican presidency or is there a misunderstanding between these two people who identify with each party in terms of what the cybersecurity threat is?

DAVID DEWALT: The way I look at this I, I wouldn't talk about it from a political point of view; a readiness point of view I will. I mean, I, I'm 100 percent certain, or 99 and a lot of nines percent certain we're prepared for a high integrity voting process. And that seems certain to me. We've done a lot of work. The Secretaries of State at each of the states, the way we've air-gapped those systems, managed those systems, double checked those systems, I feel really good that who votes is the right people voting with the right authentication and we will get a true count of who voted. So, I feel good about the integrity of the election process. I don't necessarily feel good about the influence leading up to that process which is still remains to be seen kind of what's all been occurring there and how much the technology companies are collaborating and working together to solve that. And did Russia or other nations come up with alternative models to be able to influence our, you know, our systems and our election process and we can kind of see bits and pieces of that pretty regularly. If you pay attention we've been making more arrests. We've been shutting down more sites, but the antagonizing is still occurring. But, you know, we thought we were there with 2016 and we weren't so we'll see. Influence versus integrity is a different thing to me. But, you know, it all depends what party you're from whether you think we're ready or not and I'm sure there will be a lot of contentious conversation post-election on the integrity and the influence again –

*** Expletive Deleted

DR. HOFFMAN: Um-hum.

DAVID DEWALT: -- because it seems like this is going to be a hot topic. The loser is going to cry integrity and influence and the winner's going to say no. That just seems like it's an obvious thing that's going to come down.

DR. HOFFMAN: So, it's kind of interesting. It seems like cybersecurity is something that is, is, has evidence in facts behind what's working and what's not, has become a partisan issue in terms of what, what people think, believe to be true or not.

DAVID DEWALT: I guess so. I mean, as a, as a cyber person I mean I don't feel that way. I feel like the forensics and the crime scene so to speak in a cyberworld leads us to evidence of who the advisories and how we can attribute. We, we don't always get it right perfectly but we, you know, without a shadow of doubt kind of feeling is what we end up getting. And that's why I was confident about China and Russia in my conversations just like I was with some of the Iranian activities or North Korean activities. We kind of know. There is what they call TDP's or these types of techniques that are being used in cyber that create a finger print of who did it, and you can get a pretty good confidence level of who the attackers are. So that part we know. But, you know, it all depends on your point of view there.

DR. HOFFMAN: I think it, it just demonstrates the many partisan divides –

DAVID DEWALT: Yeah.

DR. HOFFMAN: -- that we're seeing in the country this, this –

DAVID DEWALT: That's for sure.

DR. HOFFMAN: -- election year. So, I'll, I'll, we're going to do a, an open audience Q and A in about 13 minutes but I have a few more questions from my

*** Expletive Deleted

students. This is also regarding a gap, but this is a gender gap. Sarah (phonetic spelling) asks: there seems to be a significant gender gap among professionals in the cybersecurity field with women only making up 11 percent of the field according to a 2017 study. Do you believe that closing that gender gap would benefit the industry and do you think the industry needs to make some sort of cultural shift to bring more diversity into it?

DAVID DEWALT: Women, I hope you go out for cybersecurity. We are thirsty for, you know, females in this trade area. There is a huge shortage of talent, period. You know, most cyber professionals will tell you that's the number one issue we have in the cyber domain right now, is a shortage of talent, period, just overall. The amount of workload that corporations have today on the cyber problem versus the amount of resource they have it's, it's, it's a big gap. And then you get to the gender gap on top of that and it's, it's, it's massive. So, I see that as a tremendous opportunity for –

DR. HOFFMAN: How do you make –

DAVID DEWALT: -- for --

DR. HOFFMAN: -- cybersecurity –

DAVID DEWALT: -- women.

DR. HOFFMAN: -- sexy and fun and interesting to –

DAVID DEWALT: There is that.

DR. HOFFMAN: -- these young college students?

DAVID DEWALT: [Laughter.] Yeah, if you learn that can you teach me –

DR. HOFFMAN: [Laughter.]

AUDIENCE: [Laughter.]

DR. HOFFMAN: I think our students learned that today. Hopefully we'll have

*** Expletive Deleted

a couple of them offer some insight in the Q and A.

DAVID DEWALT: Here's what I love. You know, for whatever it's worth. I, I love the mission of it all. I mean, I fell in love with the industry sector of cybersecurity because in a lot of ways, yup, capitalism was working really effectively, the market grew, you know, 100 billion over a decade kind of range, and we have this massive opportunity for wealth creation but you have this great opportunity to, you know, solve a world peace problem, like a, you know, a real world issue. And if we can catch bad guys and we can catch the attackers and we can create integrity in the systems it feels like such a worthy cause. So, that's what really attracted me, and I don't think there's enough professionals out there who, you know, who have gotten educated to that opportunity. It's like solving cancer. You know, you go into the medical field because maybe you have a vision of one day solving, you know, something like that. Here you have a similar opportunity. It's a fascinating field. And it's a unlimited opportunity field. I mean, does anybody think our risks in cyberspace are going down?

AUDIENCE: [Laughter.]

DAVID DEWALT: Like, you know, this market could exponentially grow again over the next decade. It probably will. And, you know, here we have an opportunity probably of a lifetime to be in it, so. Lots of encouragement.

DR. HOFFMAN: You know, there's a lot of researchers show that the CSI shows have increased – you've mentioned forensics, it just reminded me of this – have increased students' interest in crime scenes and forensics. We need like a CSI for cybersecurity detectives --

DAVID DEWALT: Yeah.

DR. HOFFMAN: [Laughter.] -- to get students interested in this because I

*** Expletive Deleted

don't think they're really thinking about this as much as, as maybe they should. And I think we saw this today when you came to the classroom and I think before we move on I, I think a lot of our college students are wondering – this is a question from Emma (phonetic spelling) I'm sorry, from Sarah – that says, you know, what do we need to do, how can we combat cybersecurity threats in our own online spheres and physical worlds? You know, these are digital natives. These are the ones who have been connected to the internet since probably they were in the womb [laughter] and you know, now that they're becoming aware of some of these threats what can they do to, and on a consumer level, to prevent them?

DAVID DEWALT: Okay. So, here's my three pieces of advice. I'm, I'm, I'll just say this outright, so you guys can all go home and think about what you could do, consumers. This is pure consumer. So, the three things you should worry about; first of all, you should worry about your identity, right? Obvious area. You know, so there's some really low-cost things you could do to monitor your identity and your, your accounts. And there's services that you can buy. Post the Equifax breach they have their service, I think its next to free if you're and Equifax user. There's a famous one called LifeLock that you might have even seen commercials on television on. For under 100 dollars a year, which may or may not sound like a lot of money, you could monitor every account for deviant behavior on your identity. It's well worth it in my opinion because any transaction that's out of the norm can be blocked and prevented and if you want to stop crime against yourself just do that. If you only did that identity protection system you've just up-leveled a tremendous amount of hygiene for your security posture. That's, that's one. The next thing that you want to do is you typically want good

*** Expletive Deleted

hygiene on authentication. So, what does that mean? You don't want anybody to easily steal your credentials, so you can get access to your identity – it sounds simple – but there's applications you can download that are relatively free that offer you a second factor or multi-factor authentication instead of just putting your user name and your dogs name or your kids name. You basically have other factors to authenticate with and then it makes it much harder for the attacker to steal your credentials because you basically have multi-factors to log into. Now the phones are starting to offer that with facial recognition or finger printing but there's also little pin codes and sequence codes that you could put in that randomize, that add another layer of authentication into your environment. That's what I do. I use a, a little app called Duo but the idea behind it is just multi-authentication to make it harder. The third area which is probably one of the biggest attack vectors consumers face is the router. Your home router. Everybody know what a router is? So, you know, some people get it from Comcast, Verizon or somebody but, you know, ultimately that little router is not a very secure router in many cases. And it's also the keys to the kingdom of your house typically. And now with all the IOT and internet of things connecting to your home you need a secure router. That's really important. Again, relatively inexpensive but if you can secure the router perhaps have encryption, encrypted traffic to your IOT devices makes it a lot harder for them to steal things from your home. And, you know, if you're anything like a lot of people now everything is becoming digital and everything is connected to the router and ultimately that creates a vulnerability. So, a secure router, identity protection and then ultimately authentication. You do a couple of things like that, a couple of hundred dollars a year. Let's just say you went from here to there in cyberspace and in

*** Expletive Deleted

cyber, you know, consumer security for relatively little money. You notice I didn't mention any virus anywhere in there, right?

AUDIENCE: [Laughter.]

DR. HOFFMAN: That's –

DAVID DEWALT: McAfee, McAfee will be mad at me, but – [laughter.]

DR. HOFFMAN: That's great advice. Thank you. Just as a follow-up before we get to the Q and A and I'll ask Parker (phonetic spelling) and Hannah (phonetic spelling) who are going to be our mic marshals to go back to the control room and get the – we have this really cool microphone, it's called a Catchbox; it's like a box you actually toss around the audience to ask questions. So, yes –

DAVID DEWALT: Okay.

DR. HOFFMAN: -- it's cool. It's cool.

DAVID DEWALT: Is it safe?

DR. HOFFMAN: It's safe.

AUDIENCE: [Laughter.]

DAVID DEWALT: Yeah.

DR. HOFFMAN: It's safe and we're safe in here. I'm hearing thunder, so we are all good and dry and warm in here so we're going to have a great Q and A.

DAVID DEWALT: It's the perfect storm coming.

DR. HOFFMAN: [Laughter.]

DAVID DEWALT: Yeah.

AUDIENCE: [Laughter.]

DR. HOFFMAN: I planned it that way. But, I wanted to follow up because my students also had questions about what – and we have several university

*** Expletive Deleted

representatives here, faculty and, and deans and things – what should universities do to help prepare students to be safe in increasingly dangerous cyberworld? What do universities need to provide students?

DAVID DEWALT: Well, I think the first thing to realize, you know, in my experience universities are one of the bigger targets for attackers so just start with that. Because what does a university have that the attackers want? Research. You know, admissions information, financial information. Typically, parents supply a lot of information to the university, wire transfer information, banking account information, lots of credential information. And on top of that, they have a lot of research or grants, and it becomes a bit of a target. And then it has one of the easiest vectors of attack typically because the students are bringing whatever technology and applications they want to bring in connecting to the network and it's a very challenging environment to protect. But what should a university do to understand that, number one. Number two, educate the students to the risks online and I don't think a lot of universities do that well enough. It's amazing after 20 years of challenges in cyberspace we only have a handful of universities with a full cybersecurity curriculum in the United States. I mean, talk about where the education gap is and the shortage of personnel. But, there's only a few in America that actually have these programs, and I'm surprised there's not a cybersecurity major that you would take, that you would get full accredited degrees in, or master's degrees in because, you know, you now have 100 billion plus market and it's a pretty sizable job opportunity. So, you know, just couldn't we build curriculums, can we create training and education at a better level, can we prepare for some of the attacks that are occurring on the universities and their endowments and their funds and things. So, you know,

*** Expletive Deleted

very interesting opportunity for, I think, universities like Delaware here to take the lead especially with the proximity that Delaware has to Washington, to New York, to a lot of high tech here in the region; a great, great chance.

DR. HOFFMAN: All right. Well, I hope we do create something like that at the University of Delaware.

DAVID DEWALT: [Laughter.]

DR. HOFFMAN: I think that would be so cool and you could come back –

DAVID DEWALT: I'll be the guest lecturer.

DR. HOFFMAN: Yeah. [Laughter.]

AUDIENCE: [Laughter.]

DR. HOFFMAN: Okay, so let's open it up to questions. I; National Agenda is also a class that students participate in and two of my students have been so kind to offer to be our mic marshals. So, it looks like Parker has the Catchbox so whoever raises their hand. Yeah, let's start, let's start with a student. That sounds great.

PARKER: Here you go.

DAVID DEWALT: I fear a really technical question coming. Uh-oh.

AUDIENCE: [Laughter.]

Q: Um, I, you know, today, or in the last few days President Trump at the United Nations insinuated that he believes that China is likely hacking into the 2018 elections and whether that's true or not doesn't, that's another thing. But, um, you talked about Russia's influence campaign in 2016. So, who do you think would be the bigger, the biggest threat to election integrity in 2018 and going forwards to 2020 would it be China, Russia, or some other threat other than the two of them?

*** Expletive Deleted

DAVID DEWALT: Hum. That was a great question. Thank you. I haven't seen any evidence again of the integrity problem. I, I don't see China attacking our election servers or that part of it. I mean, that's just my visibility. I mean, it could be happening. I just don't see it from all the companies I'm involved with. I doubt that's occurring. That would be almost an act of war. So, the influence is a little different issue and I think there's a number of nations that have an agenda to influence America to its agenda, and I think we're seeing more and more of that. Certainly, Russia has been caught doing it, but I know that Iran has been pretty active in this area, China's been active in this area, other nations are active because again, the viral nature of the social platforms and the lack of law enforcement around this or laws doesn't say its illegal necessarily to do. So, a lot of governments are involved with that today. And it's just something we're going to have to come to grips with is what is our laws about foreign countries influencing Americans in a particular direction culturally or politically. I mean, we've never really seen this before so is it illegal [laughter]? Do we, do we declare that some, you know, war kind of act? Is that, you know, a slap on the wrist, is that a tariff, is that a what? But, we're coming to grips with that challenge right now in terms of what we've done. But, one thing I will tell you that I fear most is geopolitical tensions almost always manifest themselves in cyberspace quickly. So, whenever we do see political tensions with another country we oftentimes see that very quickly show up in cyberspace in American companies or countries and things. So, that's what you worry about particularly with the Iranian comments. We've seen more activity from that actor. We've seen other activities. We saw a lot from North Korea what they call the Lazarus Group before. Now that abated a little bit more. They went after South America's

*** Expletive Deleted

markets now to kind of keep working on their skills. So, you know, it's a, its an ever-changing political environment but the tensions create a lot of cyberspace activity quickly.

DR. HOFFMAN: It reminds me of that game RISK.

DAVID DEWALT: Yeah.

DR. HOFFMAN: Like the, you know, there's all these different powers that are, are kind of vying for – and, and a question came up earlier today that I thought was interesting which was should; would a potential cyberattack have the same or additional impact as sort of what we know now as a, a potential 9-11 or something like that? Could, could a cyberattack against this country be as big as a 9-11?

DAVID DEWALT: I believe so. I, I believe and I, I talked about this with your class a little bit, but, right now the capability we believe the number of countries with strong cyber weaponry now is about 30; 29 countries in the world have a what we think of as a strong posture for cyber offense. And, the capability is very high now in my opinion to perpetrate some sort of infrastructure attack. The question is, is motivation there? And, is the ability to be motivated to do it with that capability. We watched that with North Korea with Sony. They got some capability. The Interview movie created motivation and they attacked Sony. We watched this with other types of attacks. When we first were putting sanctions on Iran we saw Iranian DDOS attacks on our financial infrastructure. Their capability was relatively low. Their motivation was high. They perpetrated those attacks. They brought down quite a bit of banking infrastructure, website infrastructure for periods of time. Now their capability is even higher. Their motivation is rising, and we see the opportunity for these things to occur. We

*** Expletive Deleted

knew Russia always had the capability through our sanctioning process and some of their motivations, they got high enough to do an attack. That's the balance we have to watch for. That's what worries me about some of the rhetoric that's being used today. You're putting more pressure geopolitically on an adversary to inflict something back that has capability. And in an asymmetric theater, as I mentioned, that worries me that we could be in harms way. I just believe we need to calm down that rhetoric quite a bit and collaborate a lot more. It just has to happen. We need rules of conduct in cyberspace like we do in the kinetic physical world. We have to come together as nations to create a more safe environment with that. But it feels like we've gotten further away from that not closer to that recently. So, I don't know how many of you remember President Obama put together a series of cyber peace treaties one of which was with China in 2015, the summer of 2015, and we literally saw a massive drop-off of Chinese attacks post the peace treaty. That was a very positive peace treaty. We also did some with other nations -- what we call our five-I counterparts -- and we ultimately slowed the amount of cyber activity dramatically through diplomatic communications and negotiations. So, you know, one man's view, boy, we have to really work on that. That's critical.

DR. HOFFMAN: All right. Let's take a question from a community member. I think Parker still has the cube, or the Catchbox. But let's take a question from someone from the community that's not a student. There's one over back there, Parker.

PARKER: Here you go.

DAVID DEWALT: They actually throw it?

DR. HOFFMAN: Um-hum.

*** Expletive Deleted

Q: Lucky I caught it.

DR. HOFFMAN: Catchbox.

Q: In the state of Maryland one of the subcontractors for our election machines is owned, the company is owned by a Russian. Senator Bill Nelson in Florida says that the Russians are in the counties, certain counties of Florida in their election base. They have already infiltrated that. I believe it was Wisconsin that 500,000 individuals their information was hacked supposedly by Russians. What type of effort are we making to protect our election machinery? Maryland has a paper ballot so there will always be a backup to what the computer is because I've read that a lot of the secretaries of states of states are very confident in their all-computerized elections, yet their software is ancient, and they don't have it appears to be the same capabilities as new software. What are we doing to protect the actual machine, the thing that registers our vote, the thing that says that you are in the right place to vote? What are we doing to protect that –

DR. HOFFMAN: Okay.

Q: -- to help –

DR. HOFFMAN: Thank you.

DAVID DEWALT: Good question.

Q: -- [indiscernible] the election.

DR. HOFFMAN: Thank you.

DAVID DEWALT: Great question. Thank you. Again, I can talk about this as a, you know, an opinion, okay, somewhat of an expert opinion but an opinion. There's been a lot of study, a lot of work pentesting (phonetic spelling) and penetration testing this equipment, the software, the hardware. I feel really good

*** Expletive Deleted

for the most part that the integrity of that voting process will be in place. I really do. And, I think we've done, you know, best efforts in this area to make sure that that has been done. Having said that, the first part of your question and comment is something that worries me. I kind of think one of our biggest risks in America right now is what I call the insider threat which is essentially human infiltration to America's infrastructure such that they could act like Americans but they're actually working on behalf of another country to perpetrate some sort of influence or some sort of crime. And, this was true of the agency and entity that was setting up the election process for the Russians and we just have such an open border, such a, a immigration policy that enabled that to occur. A lot of breaches that occurred over a number of years was all about stealing credentials and personal information, healthcare records, even the OPN was breached with all of our classified clearances such that foreign nations could replicate and put in place personnel in America. So, until we eradicate some of that insider threat it's going to be hard for us to see what's coming in terms of the problems that may end up resulting in this. But, software, hardware, machinery I feel good about. Who operates that machinery and the human behind that is what you probably worry about a little bit at least from my perspective watching that because in many cases for me I've see a lot of insider threat, what looks like an insider threat. This is an employee already hired by the firm that is actually perpetrating from within. It's not an outside-in hack, it's an inside-out hack. And I talk a lot about one of the education problems I see right now I'm not as fearful of an outside-in hack as I am and inside-out, and, occurring from the inside out as a human inside this enterprise and that keeps me up at night right now. How to solve that problem because there is no amount of technology I can actually

*** Expletive Deleted

deploy to really understand that. I actually have to study human behavior more and I've got to monitor the humans inside the company more in order to see what deviant behavior they might be doing. But we've always trusted those employees. We've always trusted that. And that's kind of what happened with the Snowden situation, and other contractors. We trusted those employees who then kind of hurt that enterprise in some way, shape or form. So, feel good about the machinery and the code; worry a little bit about, you know, the human side of things right now especially with radicalization and other influences we've seen too.

DR. HOFFMAN: Thank you. All right. Hannah's got the Catchbox so is there a student that has a question?

DAVID DEWALT: Is there a cheery optimistic question?

AUDIENCE: [Laughter.]

DAVID DEWALT: I mean –

DR. HOFFMAN: Yeah, cheery optimistic question? [Laughter.]

DAVID DEWALT: [Laughter.]

Q: So, earlier in class you alluded to the fact that paper money might be obsolete within the next five years –

DAVID DEWALT: Hum.

Q: -- and I was wondering if you could elaborate on that a bit?

DAVID DEWALT: Yeah, one of the, one of the comments I made was just watching the change in our commerce systems right before our eyes. It's just so fun to watch. The, the, the speed of which our commerce is operating, the types of cryptocurrencies we're starting to see, the affects of them, and, I mean, we're just in a race to a virtual currency model. It seems pretty obvious to me. The

*** Expletive Deleted

question is what year is it going to be but you know, certainly a lot of, a lot of adoption is occurring quickly. The question will be is how, how sustainable is block-chain technology under some of that to really make it more secure. A lot of debate. We could talk all night about block-chaining and some of the authentication encryption techniques that that can bring. But ultimately it feels to me like commerce is going. I asked some of the students, I said how much cash do you guys all carry and like how much – well we don't have any cash. So, you know, and everything's pay by Apple Pay or something online already. I mean you can just feel the movement in that direction. So, I guess that's a fun thing. You don't have to carry cash around.

DR. HOFFMAN: Now, see, I like having some cash.

DAVID DEWALT: Don't let your battery run out but –

AUDIENCE: [Laughter.]

DAVID DEWALT: -- other than that. [Laughter.]

DR. HOFFMAN: All right. I think we had a community member with a question over here, Hannah? Thank you.

Q: There's a lot of talk about the dark web and –

AUDIENCE: [Laughter.]

Q: -- where does the dark web fit into all this thing in terms of cybersecurity as a threat or is it just activity?

DR. HOFFMAN: Thank you

DAVID DEWALT: Yeah, that's a great question. Thank you. Sometimes I, like, the question was asked to me earlier it was like what's the biggest misperception, word, or, you know, and I used dark web, dark net as one of them because there's like, ooh this thing called the dark web that everybody goes to and it's not

*** Expletive Deleted

really the reality. I mean, the reality is there is some infrastructure under these tour routers that creates some obfuscation of who you are when you're in certain sections of the internet. But, you know, basically, you know, that's not a term that's reality, is people really dealing on the dark net necessarily. But there is a lot of obfuscation that occurs for people's activities that kind of is perceived as the dark net or dark web. But, what we probably have to worry most is, you know, I feel like that privacy thing is my biggest single concern for cyber. Privacy means I can't implement security in a way that I can see behavior that looks like it could be criminal whatever internet infrastructure that's under. And I'm not saying the privacy is not good because we talked about this earlier with the, with the school as well which is in a lot of ways I don't want advertisers tracking every cookie on every browser and every move I make. I want to be able to opt in on that, not necessarily, you know, allow them to do that. So, there's some really positives but the more privacy control gets put in place, the less security we can create in, in any, in any area. Good question. Thank you.

DR. HOFFMAN: Can you elaborate on that because I found that so interesting. I don't, don't, don't know if that ever occurred to me before that more privacy means less security.

DAVID DEWALT: Um-hum.

DR. HOFFMAN: Could you elaborate on that idea?

DAVID DEWALT: Yeah, I, I mean, in a lot of cases some of the behaviors that we'll see online as a result of the trail, the breadcrumb trail helps us understand was it really you sitting in this chair with your phone turned on located in this hall, in this – yeah, exactly. That behavior if I track it I know it's Lindsay Hoffman sitting right here –

*** Expletive Deleted

DR. HOFFMAN: Um-hum.

DAVID DEWALT: And not an operator in Moscow acting as Lindsay Hoffman.

DR. HOFFMAN: Um-hum.

DAVID DEWALT: And, so, the more of that I can gain access to the more I can validate that you're the real person and allow you to log into the, the network.

DR. HOFFMAN: But the more privacy I have that limits you from seeing –

DAVID DEWALT: Right.

DR. HOFFMAN: -- where I am.

DAVID DEWALT: Right, exactly. So, one of them would be an IP address obfuscation which you're not allowed to see what IP address I'm coming from or what internet protocol address I come from. If you block that I can't tell what location, you came in from. Now I don't know what country you came from. And, suddenly, you know, there's issues that can, can occur from that. So, the more I can gain access to I can't let the privacy block us from all of that. So how do we create balance? That's the key. You know, we want enough privacy to have our freedom, but we want enough security to feel protected. Wow is that a fine line and it's super hard to do.

DR. HOFFMAN: Would you say we are on the far end on privacy where as China is on the far end for security?

DAVID DEWALT: Yeah.

DR. HOFFMAN: Yeah.

DAVID DEWALT: Yeah, I talk a little bit about that. I mean, look in what privacy rights do you really have in China with the way their architecture works, not much. Here we have a tremendous amount of privacy for the most part and, you know, we're on two ends of that spectrum. So –

*** Expletive Deleted

DR. HOFFMAN: All right. Sorry, I'm jumping in on the audience question time.

DAVID DEWALT: [Laughter.]

DR. HOFFMAN: This is just such an interesting topic to me. So, Parker's got the Catchbox again. So, anyone over on this side? Yeah, right in the middle there. And, Amelia (phonetic spelling) can go next. She's been waiting.

Q: Um, sorry, um, I just want to make a comment on what you, something you said earlier. My name is Charlie Bonsalatt (phonetic spelling). I'm a professor here in Electrical and Computer Engineering.

DAVID DEWALT: Okay.

Q: We do offer a cybersecurity minor to undergraduates. They could go to the UD catalogue and look up the department and find it there. They can always come to the department and ask questions too. We also offer a master's degree both online and on campus in cybersecurity. So, I just wanted to –

DAVID DEWALT: Thank you, Charlie. Awesome. Good --

DR. HOFFMAN: I'll make sure I post –

DAVID DEWALT: I'm sorry I didn't know that –

DR. HOFFMAN: I'll make sure to post that with the video that goes out tonight.

Q: Okay.

DR. HOFFMAN: Thank you so much.

DAVID DEWALT: All the females in the room sign up with Charlie right here.

AUDIENCE: [Laughter.]

DAVID DEWALT: There you go.

*** Expletive Deleted

DR. HOFFMAN: All right, we have another student question right in the front row here, Parker.

Q: Sorry, okay. You were kind of just touching on this, but you were saying that as Americans we prefer our privacy over security and, but, we've seen in the past couple of years that our privacy on social media has posed a threat and has actually produced physical violence. Like for example, the shooter at Parkland High School this past February posting his threats on Facebook. So, do you believe social media platforms have a responsibility to work with the government to censor and prevent things like this from happening? And, what do you think that role should be? It's a hard question.

DAVID DEWALT: Yeah, that's a hard question. A little what I answered earlier was, you know, again a lot of these social platforms aren't beholding to law or ideology for being forced to work with government on this. They can decide they want to, or they don't want to. Apple made that clear. I think others decide based case by case. So, my personal opinion is, they should. I mean, in these particular cases where the safety of our citizens and around the world every country that you do business in you should have that same policy. If the government needs help because of a harmful situation we should have that responsibility to help. That's my opinion. But, in many cases a lot of, a lot of belief is that that privacy is so important that they will protect it all the way down to not allowing access to a phone or to a social media account. So, each corporation is a little different on the way they look at that unfortunately. Yeah, it's a good question.

DR. HOFFMAN: All right. It looks like we've got a question in the back.

Q: Yeah, my name is Atol Kai (phonetic spelling) and I'm the

*** Expletive Deleted

interim director of the Cybersecurity Initiative. And, glad that Charlie answered some of your issues you raised. But, there are two tests we are doing, we are planning to do now. First, to introduce cybersecurity to non-stem (phonetic spelling) majors so that everybody on campus will have some background in cybersecurity. Not only for stem (phonetic spelling).

DR. HOFFMAN: Um-hum.

Q: And another thing we are doing now is that we are trying to introduce a blockchain also as a class for everybody across campus. And like I saying, the material science and physics we're also working with them to introduce a quantum computing because you know the Russians have started working on quantum computing in the blockchain and the issues it will bring. So, we at the university, we've already started talking and then I think by next semester we'll have a strong program both in the blockchain and then the quantum computing aspect so that we can fight against the future threat. Okay.

DAVID DEWALT: Love it.

DR. HOFFMAN: Thank you.

DAVID DEWALT: And I know we're also here at the university a whole series of data science projects cutting across the colleges as well and uniting that. That's a very encouraging development and I'm proud of the university for, for all of that. So, I really –

DR. HOFFMAN: Yeah, we're, we're definitely on the cutting edge and I'm, I'm proud that the Cybersecurity Initiative is, is cosponsoring this event tonight, and I'm hoping that as I talked with some engineering folks at dinner that we can start introducing ideas to the social sciences, to the humanities and to other parts of the campus that might not even be aware of some of these issues. So --

*** Expletive Deleted

DAVID DEWALT: Yeah.

DR. HOFFMAN: -- let's make UD the next, like, cybersecurity aware campus.

[Laughter.]

AUDIENCE: [Laughter.]

DR. HOFFMAN: All right.

DAVID DEWALT: I'm going to add on one comment there if I can just for a second because it's really important to what you were saying. I mean, cybersecurity in general is like an education foundation but I would really encourage the university from an education point of view to pay attention to where the biggest risks are at right now in the cyberspace and how do we get this youth movement to help us with this problem. We already talked about the social networks and issues there but there are some other areas that it, it just hurts my head that we're not creating advancements in for the safety and security of our nation and our world. I'll give you two examples real quick that I've been very, you know, passionate about. One area is drones. So, does anybody think drones are a problem right now? You should all raise your hand.

AUDIENCE: [Laughter.]

DAVID DEWALT: Because last Christmas 3.5 million drones were sold and we're going to see exponential growth of drones. And what is monitoring behavior of drones right now? How much explosive device could be loaded on a drone? Why buy an assault rifle with a bump stock if I can go down to the local electronics store, buy a drone and fly the drone into a stadium or an airport or a physical facility? Right? So, we have to move fast in this area. And, some of you might have seen the Venezuelan president's situation that, you know, narrowly missed killing the president and a lot of the staff there. It did kill people.

*** Expletive Deleted

But, I mean, this is a real problem, and this isn't our cyber network. This is our cyberspace above our physical facility that needs to be protected. So, how do we begin to solve that problem? I got involved with a couple of companies, but there's like two or three companies in the world working on this and they're all this big. And so, we need inertia to solve that problem because the drones are creating a massive problem. On top of that, Amazon and Google and others are now going to be delivering, building beehives, what they call beehives. So, a beehive is a ground station with up to 3,000 drones that can fly around that delivering packages to your doorstep. So, if we don't build security hardening into those systems and help in that way we are going to miss another significant problem. And, I've been talking about this trying to get the FAA and others just from transportation industry to engage in this area. Another educational platform opportunity to do. The other one I talk quickly about is our satellite control systems and one of my biggest fears is watching – right now there's I think through 2017 coming this year 1,572 – I'm usually pretty good with numbers – 1,572 orbiting, earth orbiting satellites. We're going to launch 3,000 more in the next 12 months.

AUDIENCE: [Whistle.]

DAVID DEWALT: So, in 25 years of satellite advancement we're going to double that number in one year because almost every industry is launching Leos and Neos now for whatever industry sector they're in. And what constellation was it launched into? What's the governance model? How much security is in it? And what critical infrastructure is talking to that satellite? And this is all using radio frequency wavelengths and other types of non-secure protocols that, again, education and what we have to do to solve that problem before it becomes a

*** Expletive Deleted

major problem is really up to us. I mean, I feel like there's enough awareness to it, but we've got to get inertia as a community to solve these problems. It was a lot like we saw, hey, here comes China. We already see it. Or here comes Russia; two years later we've done nothing about it. And that's a shame because we can see the drone problem and the satellite problem coming, at least I can. And I've been trying to educate wherever I go to these types of issues that are happening and we've got to go solve them. So, anyway, a longwinded way of – maybe we can have a droning class too.

AUDIENCE: [Laughter.]

DR. HOFFMAN: I was hoping you weren't going to talk about the drones.

DAVID DEWALT: [Laughter.]

DR. HOFFMAN: [Laughter.]

AUDIENCE: [Laughter.]

DR. HOFFMAN: Hearing about them earlier was frightening enough. All right, I think we have time for one more question. So, Parker's got the Catchbox. Ooh, it's a far one. Can you throw it all the way to the woman in –

DAVID DEWALT: Oh-oh.

DR. HOFFMAN: -- the center?

DAVID DEWALT: Don't hurt anybody.

DR. HOFFMAN: Yeah.

Q: Yeah. So, you've been talking about nation states having the resources and capacity to, to launch these kinds of attacks. Are there non-state entities that also have this capacity or are developing this capacity? Just so none of us get any sleep tonight.

DAVID DEWALT: [Laughter.]

*** Expletive Deleted

DR. HOFFMAN: [Laughter.]

AUDIENCE: [Laughter.]

DR. HOFFMAN: Thank you.

DAVID DEWALT: Yes, there are. There's quite a few. In fact, one of the techniques a lot of the large countries have done was set up operations to look like it's a criminal group or some sort of activist group or a terrorist group as a pawn to the larger chess game that they're playing. So, it's another cyberspace problem is now we're setting up entities and agencies and operations that are really government backed but they're now sitting in Northern Africa and not Russia, or they're sitting in another location. And so, a little bit of the challenge we have is that kind of problem with smaller groups still motivated in a different way and now we're watching some of the ISIS kinds of environments starting to get cyber activities too. Should we end on a cheerier note? Like –

AUDIENCE: [Laughter.]

DR. HOFFMAN: All right, let's – what's one –

DAVID DEWALT: You better come up with a better one.

DR. HOFFMAN: Let's, like let's end with what's one really cool technology, a really positive [indiscernible] –

DAVID DEWALT: I had a really cool idea today for your athletic director. I'll tell you that one.

DR. HOFFMAN: Okay.

DAVID DEWALT: Yeah.

AUDIENCE: [Laughter.]

DAVID DEWALT: So, here was my idea, maybe I'll scare you after this conversation, but I was like, all right, so, you know, we need, we need our

*** Expletive Deleted

mascot to be more present, right? The Blue Hen? So, as I, I started I'm like okay it's the Fighting Blue Hen and we need like, you know, a lot of universities run the buffalo out on the football field or fly the falcon into the, land on the arm. It's something. Like, we need like a marketing presence of our Blue Hen. But I learned today that the Blue Hen is kind of really like a fighting blue hen and it doesn't really cooperate well on a football field or –

AUDIENCE: [Laughter.]

DR. HOFFMAN: [Laughter.]

DAVID DEWALT: -- a basketball court, right? So, I think we should get a custom blue hen drone.

UNIDENTIFIED: We have some [indiscernible] –

AUDIENCE: [Laughter.]

DAVID DEWALT: And that blue hen drone will be a beautiful drone that we can operate –

DR. HOFFMAN: You want a drone?

AUDIENCE: [Laughter.]

DAVID DEWALT: No, we're going to get a simulated –

DR. HOFFMAN: [Laughter.]

DAVID DEWALT: -- fighting blue hen drone. It flies in, does all kinds of music and colors at the stadium and is going to be the first mascot drone in the United States and it's going to show our technology savviness painted exactly like a blue hen and it's going to cooperate really well.

DR. HOFFMAN: [Laughter.]

AUDIENCE: [Laughter.]

DAVID DEWALT: Come on.

*** Expletive Deleted

AUDIENCE: [Applause.]

DAVID DEWALT: That's a good idea. Marketing. I'm not sure she liked it or not but anyway.

DR. HOFFMAN: Well, now it's, now it's going to get out there.

DAVID DEWALT: There you go.

DR. HOFFMAN: This is going to go viral.

DAVID DEWALT: It'll go viral.

DR. HOFFMAN: We'll see what happens. Well, before we say thank you to University of Delaware alum Dave DeWalt for being here, I wanted to make a few points just before we go. I'm really excited. Yesterday we had, it was National Voter Registration Day and we had over about 200 students, new students register to vote in Trabant.

AUDIENCE: [Applause.]

DR. HOFFMAN: And, since September 1st we've had almost 500 students, or actually almost 600 students register to vote and it, having come to this campus in 2007 when we were rated one of the most politically apathetic campuses in the nation it's really exciting to see students getting so involved. So, thank you students for, for being here and for registering to vote.

AUDIENCE: [Applause.]

DR. HOFFMAN: If you haven't registered or if you want to get updates about upcoming elections you can go to udel.turbovote.org. It takes only a few minutes to sign up. Tell your friends. I also wanted to make sure that you guys know about the Delaware Debates, October 17th. It's a free event but you do need tickets for it, so you need to get, go to the box office at Trabant to get tickets for that. You can find out more information at delawaredebates.org. We have a

*** Expletive Deleted

living room conversation coming up on October 25th. This is where we'll have students from both the college republicans and the college democrats as well as some other students engaged in voter engagement efforts talking about why its important to vote. Thank you.

DAVID DEWALT: That could be a lively debate.

DR. HOFFMAN: Yeah, yeah. So, it's, it's to demonstrate how we can actually have civil dialogue even if we might disagree with each other. It's possible, it truly is. I've, I had John Kasich and Joe Biden on this stage and they got along very well. So, finally the Voices Contest – I've mentioned this a few times. We have an audio essay contest that students can enter to talk about why their voices matter and what matters to them particularly in this election and talking – the theme for this year specifically about free speech, hate speech, things like that. So, the last thing that I'll announce here is that we have our next speaker. I think I'm, I don't know if I told you thing, our next speaker is a 16-year-old –

DAVID DEWALT: Oh, yeah, you mentioned.

DR. HOFFMAN: -- who is, started his own email update about politics called "Wake Up to Politics." I actually highly recommend it. It's a very non-partisan update on what's happening everyday on the Hill. He did have to take a break over the summer when he went to summer camp.

AUDIENCE: [Laughter.]

DR. HOFFMAN: Um, so, we, we had a month of no "Wake Up to Politics" --

AUDIENCE: [Laughter.]

DR. HOFFMAN: -- but he has almost 60,000 subscribers including, you know, well known journalists and politicians. So, he'll be here October 10th. It should be a very interesting discussion. And, finally again, I want to thank the

*** Expletive Deleted

Cybersecurity Initiative for cosponsoring the event and I really hope that we can coordinate on some future efforts as well. So, please finally join me in saying thank you so much to Dave DeWalt for being here.

DAVID DEWALT: Thank you. By the way, real quickly, I just want to thank Dr. Hoffman here. She's doing an amazing job. I really appreciate everything you're doing.

AUDIENCE: [Laughter.]

DAVID DEWALT: Great class and thank you. Awesome to watch you. Good.

DR. HOFFMAN: Thank you. All right.

DAVID DEWALT: Thank you everybody. Good night.

DR. HOFFMAN: Good night.

# # #

*** Expletive Deleted