FDD EVENTS

Engineering the Solution to Critical Infrastructure Cyber Sabotage

Introductory Remarks by Clifford D. May
Featuring Andy Bochman, Sarah Freeman, and Andrew Hildick-Smith
Moderated by Samantha Ravich

MAY: Hello, I'm Cliff May, FDD's Founder and President. Thanks for joining us today. For those of you who may not be familiar with us, FDD is a non-partisan research institute focused on national security and foreign policy.

I'm pleased to welcome you to today's event on Consequence-Driven, Cyber-Informed Engineering hosted by FDD's Center on Cyber and Technology Innovation. CCTI seeks to advance U.S. prosperity and security through technology innovation while countering cyber threats that seek to diminish it. CCTI promotes a greater understanding within the U.S. government, private sector, and allied countries of the threats and opportunities to national security posed by the rapidly changing and expanding technological environment.

Today's event will discuss a vitally important topic: the vulnerabilities posed to America's critical infrastructure. More importantly, the experts and practitioners with us will discuss well-researched solutions and methods that public utilities and policymakers could implement today to better counter cyber sabotage. The concept of Consequence-Driven, Cyber-Informed Engineering was developed by Andy Bochman and Sarah Freeman, who are both joining us today. A link to their book on this methodology is on the events page.

Andy is the Senior Grid Strategist for Idaho National Laboratory's National and Homeland Security directorate. Sarah is an Industrial Control Systems cyber security analyst at Idaho National Laboratory. We also are pleased to have Andrew Hildick-Smith joining us. He worked at a large water and wastewater utility for 30 years and is currently the Water Sector Chief for the Boston section of InfraGard and a Principal at OT Sec, LLC.

Finally, my colleague Samantha Ravich will moderate today's event. Samantha is chair of FDD's Center on Cyber and Technology Innovation and its Transformative Cyber Innovation Lab. She also serves as a commissioner on the congressionally mandated Cyberspace Solarium Commission.

We hope you enjoy today's conversation. I encourage you to learn more about FDD and check out our recent events and analysis at fdd.org. You can follow us on Twitter @FDD. I am now pleased to turn the floor over to Samantha.

RAVICH: Hi, we're here to discuss Consequence-driven Cyber-informed Engineering, or CCE, and the vulnerability of critical infrastructure to disruption by cyberattacks and to congratulate Andy and Sarah on the publication of this great book, and I highly recommend it. This topic of the vulnerability of critical infrastructure is finally starting to get the attention of the broader public. Of course, the folks on this panel have been studying this issue for many, many years and how to mitigate the problems, but I do want to reference that even the World Economic Forum noted in its 2020 report that cyberattacks on critical infrastructure now are rated the fifth top risk to the global economy.

So, let's get into it. Let me first turn to Sarah. Tell us a little bit about the origin of the concept of CCE, and how did you come to recognize the challenge facing critical infrastructure and the need for engineering solutions?

FREEMAN: It's interesting, because a lot of what you were just saying there really speaks to the heart of the origins of CCE. At Idaho National Laboratory, we spend a lot of time looking at critical infrastructure protection issues, and much of that is threat informed formed. So, as we've seen more and more examples of advanced attacks against critical infrastructure, or even advanced attacks that could be applied to critical infrastructure, it became apparent to the group that there was a disconnect between what defenders thought the attackers were doing and the degree and sophistication skill that they were demonstrating. And that gap between defenders and attackers was something that we were really trying to address with CCE.

RAVICH: Great. Andy, now that we kind of understand why CCE was conceived in the first place, can you tell us how it works and what makes it different than traditional forms of cyber defense, which are really focused on patching vulnerabilities, strong firewalls, air gaps, and other digital solutions?

BOCHMAN: Yeah, sure. Sure. I just want to say, first of all, it's a pleasure to be with you guys today. Thanks. Thanks for this, Sam. Yeah, it definitely goes against, I think, a lot of the common wisdom of what the cybersecurity industrial business has form – what's formed around it. It looks first to engineering rather than to adding more digital technology on top of what we already have as everybody's modernizing. There's four basic phases to it. But one constant theme throughout each phase is, "Think like an adversary." A colleague of ours, Marty Edwards, who's given talks on CCE in the past, coined the phrase, "Think like an adversary, but act like an engineer."

And as you go into the first phase, and I'm not going to go into too much detail, that can be done on people's own time. But as you go into the first phase, we're trying to identify the comparative handful of functions and processes in an organization, could be an industrial company, perhaps, it could be water, it could be electricity, ONG, chemical, et cetera, it can be the military sometimes too.

But what are the handful of essential functions and processes that simply must not be allowed to fail, that would cause a strategic business risk, corporate viability in the business world? We have a method of running scenarios that helps us tease those things out. Often the organization has a sense for what some of those things are, but because they've spent very little time thinking about how to kill themselves, they haven't gone to the level of depth that we help them get to and flesh that out. Then we take it through a mapping of the entire digital ecosystem that supports those functions, not the whole enterprise, not every end point, not every network or application, but the things that support those most critical, cannot-be-allowed-to-fail functions and processes. That's phase two.

Phase three, this is something Sarah is particularly adept at, is targeting. How to craft using ICS or other cyber kill chains, how to get through that landscape to ultimately create the payload that causes the unacceptable effect that we're all trying to avoid. We usually rack and stack those by how easy they are, that choreography to how to create that catastrophic effect, sabotage, if you will, how confident you are and how many steps it requires.

Phase four is the last one. It's called mitigations and protections. And here, like I said at the beginning, is where we turn first to engineering first principles, things that we've used to build bridges, roads and buildings for centuries based on physics. And I think we'll get to it shortly, but we have a fairly topical example to help flesh this out, using that unfortunate water utility in Florida. We'll get to that, I think.

RAVICH: That's great. And I really liked that phrase, "Think like an adversary, act like an engineer." But you and I have talked that this isn't only for engineers and operators, the whole concept of CCE. So, why is it actually, and why is it critical for a wider range of stakeholders to understand the solution? And what conversations do you want to be occurring at the board level, in the C-suite, to get them in the mindset of, "This is a way to mitigate some of the largest vulnerabilities that they're going to be facing as we go forward?"

BOCHMAN: Yeah, those poor folks at the board level and the senior executives and all, whose day job is not cybersecurity, it's to run a successful business and, ideally, grow it. In 2021, they now have a senior person in charge of cybersecurity, in my opinion, ideally, IT and OT, cyber and physical. They usually lump in compliance too. And they're hoping, they're really hoping, that that person is doing a great job. But it's such a hard thing. It's a hard thing to know

whether you have enough of the right kinds of security, whether you're ever making any mistakes that are leaving doors open for adversaries.

The thing that we can talk to those folks, and I also think of folks at that level as being similar to their peers, if you will, on the Hill, the members in the House and Senate and their staff too, again, such an abstract concept. CCE is a way of making something that's so ineffable much more tangible.

If you show what the mitigation is that protects the large turbine from killing itself, if it's instructed to do so by digital means, if you show blueprints for how you've sized certain vessels that are holding caustic materials that could cripple your business if they were ever released all at once by destroying long lead time to replace capital equipment. If you look at these diagrams, we can just use what we've known, what we've learned as a civilization to say that "Even if this thing was told to kill itself, your cyber insurance isn't going to help with this, by the way, typically. It's going to get into the realm of your catastrophic loss, property loss types of stuff." Then folks can have a lot more confidence that they are as protected as they hope they are. They hope that their cybersecurity program is protecting them.

And one quick add on, please, please know, we are not advocating for stopping doing what folks are already doing in terms of, the book describes it as "cyber hygiene," but by that, we mean the sum total of all the activities, all the products they bought and deployed, all the training they put themselves through, all the expert consultants that they hire and outsourced security providers. Please keep doing that to the very best of your ability. It's just, we're saying, "At the end of the day, there are certain types of adversaries that can find their way through those things. And if they do, and when they do, there are some things you can now do to make sure that the very worst things don't happen."

RAVICH: Yeah. No, that's great. And actually, one of the quotes on the back of your book is from Tom Fanning, who is CEO of Southern Company. He sits with me as a commissioner on the Cyberspace Solarium Commission. And I love what he wrote, he said, "At its core, CCE is really about keeping operations going no matter what adversary nations or hostile groups have up their sleeves." So, that's at the strategic board, C-suite level of thinking that then can get those others in the company to really take these steps.

BOCHMAN: Absolutely.

RAVICH: Andrew, let's turn from the concept to reality. And you were one of the earliest adopters of CCE while you were at a very large U.S.-based water authority. What made you latch onto this solution and how did you convince your colleagues of the necessity and the utility of the solution?

HILDICK-SMITH: So, for us, I mean, we always worried about the control system and its security, but after the release of information about Stuxnet, and in particular, a presentation by Ralph Langner on the details, it was very clear that even though we were trying to do a good job with cybersecurity, we weren't going to stop somebody who was talented or determined. So, then we started looking at it in terms of, "What could go terribly wrong by somebody breaking in?" We'd looked at that just in terms of operator errors and things before, but never from a point of view of cybersecurity, somebody intentionally doing damage. So, in 2013, we had put together just a very small task order contract to have to protect some pipes from getting over pressurized by having too many pumps go on. But it wasn't obvious to the person who needed to approve that, so it just languished for a little while.

And then the next year, there was a talk by Jason Larson that reinforced the possibility of somebody attacking with a bad intent and possibly damaging your infrastructure, so like the critical aspects, processes that Andy was talking

about. So, then that led us to do some internal system modeling that we could justify what we were saying, and then that was implemented through a capital contract, and then subsequently installed at other pump stations by in-house staff. So, it was a baseline worrying that took a big jump up when it was clear that the cyber hygiene and all the good things you can do just wasn't going to be quite enough.

RAVICH: Yeah, that's great. It's so thoughtful, because it's just easy to say, "We'll just do business as usual," even when business as usual is completely failing in terms of mitigating vulnerabilities. So, to break with the past and say, "We have to think about this problem differently if we're going to face this different kind of battle space that is really heating up." So, really, really fantastic, fantastic work. Andy, did you want to say something?

BOCHMAN: Yeah, I was just going to say, there's a phrase that we use in public and also in the book that basically says, "It's not a good idea to rely on hope and hygiene." Hope and hygiene. Hygiene, again, being the sum total of everything you're doing now. And then I just hope that on my watch that they don't come calling for us. I learned in earlier business classes that hope is not a strategy. So, this is something more concrete, something that you could sleep more soundly with.

RAVICH: Yeah. Yeah, no, absolutely. And, again, what's hitting the press in terms of attacks on our critical infrastructure, it should actually be keeping more people awake.

So, Andrew, on that note, let me follow up with you, because, as I said, cyber vulnerabilities of the water sector, specifically, are receiving front-page coverage, following the attack of the water treatment facility in Oldsmar, Florida. So, you might want to talk a little bit about that. Something that when we were talking the other day and I heard you say was really interesting and I think is going to be counterintuitive to many people listening to this panel, which is that the water sector actually has some advantages over the electricity sector when it comes to implementing cybersecurity solutions. So, maybe take a few moments, walk us through Oldsmar, and, of course, if Sarah and Andy want to jump in on that discussion as well. But then also what you were schooling me on about some of the advantages in the water sector.

HILDICK-SMITH: Yeah. So, I'll start with that water versus electric sector. Just the water sector, things happen much slower. So, you can have a pressure wave that's very fast, but generally everything you do is paced, and as a water utility, you're typically not connected to any other utilities, which is opposite of what's happening in the electric sector. The electric sector has ISO's and other groups that link everything together. So, it's an extra layer. Like if you're in a water utility, you can do pretty well at isolating. Isolating doesn't mean you're free from somebody attacking you, but it's one step in a good direction.

What I just wanted to say, the thing about the CCE that I think is really great is in particular the phase one, where Andy was talking about identify those critical processes. And then the phase four is coming up with physical solutions that can protect your process. If somebody breaks in, or at the same time, if an operator makes an error or something else goes wrong, it's protecting your process. And in those two aspects, you don't have to be a cybersecurity wizard. You can be the engineer; you can be a maintenance person. There are all sorts of people in a water utility that can successfully work on those two steps and make a real difference, which is really exciting. So, you can have a small utility that comes up with a really great solution on its own and they can keep doing those cyber hygiene items. But they have in-house staff that are the experts on their process. So, that's really cool.

Jumping to the Oldsmar case. That was interesting because – just as a quick summary, somebody broke in and adjusted the sodium hydroxide level of the caustic to adjust the pH and essentially dialed up the level way high up to

11,000 parts per million. And maybe the process couldn't even achieve that, but the intent for human damage was there. And it echoes something that happened in 2007 in Spencer, Massachusetts, where it was an error and it's a similar sized water system that accidentally released sodium hydroxide over the course of the night. And then when their pumps started up, it released it into the water system. And there were about a hundred people that had to go to the hospital from taking showers or physical burns, and at least one person had damage to their esophagus. And so, it was a scary thing.

And in that phase four the CCE could help any utility. And in that Oldsmar case, there are a few things that you could do to improve the resilience. So, one would be just having an independent monitoring system separate from your SCADA system. So, you can get an alarm. If the SCADA system is compromised, something else can give you alarm that there's a problem. You can do that engineering solution by having a relay contact off of the pH transmitter. That's what's monitoring the level of the sodium hydroxide that will cut off those sodium hydroxide pumps if it's seen a level that's too high. So, that can, again, be independent of the SCADA system.

You could change the pump size. So, the pumping, it's a fun – I don't want to go into too many details. But it's a small amount for – I don't know how much was released actually, could be released at Oldsmar. But in that Spencer case, it was only 34 or so gallons, it's a small amount of liquid. And so, you might be able to redesign the pump size so it's smaller or change the capacity of the container. It all depends on how their pattern of treatment and flows to their tanks. But anyway, there are things that you can do to prevent that kind of water quality problem, or physical damage to systems.

RAVICH: Yeah, and I want to turn to Andy, I think he wants to jump in a little bit on this. And I know you were going into detail, but actually I don't mind, and I don't think our listeners mind because in most of our cybersecurity discussions that we're having around Washington, the broader policy community, we have to put our heads in our hands because where do we even enter into the discussion to find any ways to mitigate? So, the fact that you just rattled off, "And we can do this, and we can do this." And there are things that can be done, is very hopeful in a discussion that often is not. So, Andy, you wanted to say something?

BOCHMAN: Yeah, sure. Just a couple of comments and I'll try to stay short. It's important to note that the things Andrew was listing there are often extremely affordable. Which is a weird thing in cybersecurity, where we think we have to go to the Moscone Center, the pilgrimage every year to the RSA Conference and find out what the new quantum blockchain solution is. It's going to be expensive, but it'll keep you safe, you hope.

These things are so practical and easy for lay people to understand. It's really wonderful. The particular remark that triggered me was when Andrew said, "You don't need to be a cybersecurity expert on this stuff in many cases." In some cases, you do, when we're at this serious national security level. Some of the INL's projects, you need the whole shebang of the methodology and connected to the intel community and all that. But from many companies, especially smaller and mid-size ones that just don't have the resources of the big guys, I almost wish that the term didn't have the word "cyber" in it. It scares people and it makes them think of all that other stuff. It would be better if it was just engineering that protects you from catastrophes. The cyber-enabled part is there simply because that's how they're going to get to you. But once you get past that, there're things you can do that really don't much background in that domain.

RAVICH: So, Andy, you mentioned the words national security. So, I want to turn to you Sarah and talk about what happened in Ukraine a few years ago when the Russian hackers attacked the electric grid. And look, we know that the Russians have tried to penetrate American utilities. So, thinking back on Ukraine and maybe give some high level points,

because I know you were very involved in the mitigation afterwards, but how would the CCE thinking through help protect against a repeat of what happened in Ukraine?

FREEMAN: Of course. So, in December 2015, and then again in December of 2016, there were a couple of incidents where externally enabled cyber actors accessed machines and systems that have been put in place specifically for normal operations. This is probably a trend that we've seen more and more of. Usually in these conversations Stuxnet comes up. But a lot has changed since Stuxnet, so not everything looks like that. Not this concept of an independently enabled piece of malware that gets inserted and then wreaks havoc.

In this case, you had external parties connecting through, in the first case, HMI's through VPNs, through normal infrastructure and then having access to that stuff operated the system as intended. So, in this particular case, they were opening breakers at the first time and it resulted in a loss of power to something like 225,000 end nodes. The customer numbers are hard to get because a specific end node might result in more than one person losing power at their residence, that kind of thing, especially if it's an apartment building. So, the numbers are high.

And then we saw a similar activity occur in 2016, but this time at a transmission level substation. So, in that case, there were a few things that came out of it. I think for a lot of people it was a real showstopper. It was really a surprising event in a number of ways. I know at Idaho we had to stop and take stock again. Doing a lot of cyber threat intelligence work, we'd fallen into the trap of evaluating things based on their level of sophistication. There were sophisticated aspects to that attack. There was a lot of coordination that went in, there was a fair amount of pre-planning. But the actual movements themselves, what the attack operators were performing, was amongst the most basic of activities. They were using the system against itself. And they did so intelligently, but this wasn't a master criminal cyber activity. And it's interesting because a lot of people want to fall into that trap. Almost that fear, uncertainty, and doubt. But it's really important that we have a realistic spectrum so that we know when something is truly devastating, and we really do need to bring everybody together very quickly.

In terms of CCE, and in fact, after we went to Ukraine in May 2016, one of the things we talked a lot about with the energy entities over there was proper responses. Because in that circumstance, I think everyone was equally shocked and there were certain things that happened that could have happened more quickly in order to limit that impact. In fact, in one of the cases, one of the distribution entities they felt empowered enough to just disconnect the energy management system, the distribution management system, and in doing so they took away the pathway the attackers were using to manipulate and control those points.

So, when you're talking about CCE, part of it is knowing yourself, and an example like 2015 and 2016 really illustrates what your stated function is, your mission goals and those kinds of things and then how it can be used against you. But I think that for most people, what we're trying to get at here is not having that failure of imagination. So, especially in the first phase of CCE, we're really trying to look at how the system can be manipulated. And so, examples like that are just very helpful for moving the conversation along. There are challenges if you look at how you move beyond that. So, if you want to say, I want to put in protections and mitigation specifically relevant to that. Obviously, we did a lot of work, both in Ukraine and the United States, to make that more feasible. Obviously the first thing, like I said, was this education. This is in the realm of the possible, how would your people respond? And do they feel empowered to make these critical decisions that change how the control system is interacting with the environment?

But even beyond that, sometimes it's a little bit challenging. In the Ukrainian case, for example, their recovery actions were very manual. They didn't trust their systems. They couldn't guarantee that they'd properly cast out the

attackers from those environments. So rather than operate potentially contaminated networks, they chose to operate at a degraded state for many, many, many months. In the United States that's probably not an option for us, unfortunately. We have adopted higher degrees of automation and we don't necessarily have the manpower to take that on. But being able to, say, quickly island operations, so that you can't necessarily have an impact that's as wide scale, looking at balancing authorities and the resiliency across the electric grid, that's all things that can be done.

There are obviously also technical things we can put in place in terms of how many virtual private network points can connect to your system at any given time. That would also challenge this, at least in the manifestation we saw in 2015 because there was a lot of activity that was going on really quickly and it was clearly malicious. So, putting in place fall gaps that say, "This is too many," or "You've exceeded the number of connection points," that's all stuff we would also encourage people to do. But the real problem here, and I think this is where – I said this already, but CCE isn't necessarily about looking at a past example or a past attack and trying to mitigate against it. We can do that, but that's kind of what we were already doing.

There's lots of entities that will tell you immediately after an attack how to better protect yourself, best practices, things you should do to make sure that you're not as at risk for those kinds of things. CCE is about predicting the next attack. And so that's part of the reason why it has this combination of threat intelligence, why it brings in the engineers, because as Andrew said so elegantly, nobody, even the attackers do not understand these systems to the degree that the engineers that built them. And so, part of the defensive advantage is bringing those people into the room.

There's a fair number of engineers who actually, for whatever reason, have already thought about what the worst case scenario would be on their systems because they've looked at them day in and day out. If you can identify those people in your organization, it's invaluable to hear how they think that their system would be destroyed. Then if you can take those that are perhaps right on the fence but show them what an adversary attack planning thing looks like, understanding how they get into your system, how they manipulate certain points, how they learn, what your weaknesses are, and you can change their perspective, then you've duplicated the number of people that we like to say have the evil bit. So, you use the evil bit for good. But that perspective, however we can get there, that's the core part of CCE.

RAVICH: Yeah. That is fantastic. And that's also just what you talked about at the Center for Cyber and Technology Innovation, which is hosting this panel. But that's why we were so excited to learn about this because at CCTI we take on the human elements that are preventing people, corporations, parts of the U.S. government from adopting best practices. That fear, doubt, and uncertainty. Is it lack of authorities? Lack of resources? Lack of, I don't know what this is, and it scares me that I'm going to break the internet? Whatever it is, we try to get underneath that to open a space or folks like you and important work of CCE to walk through. Andy, I know you wanted to jump in for a moment.

BOCHMAN: Sure. Yeah. Just as the tail end of Sarah's description and then your pivot into the human element at FDD. While CCE is entirely science-based the description of taking somebody who's on the fence and they're like, "I don't know if anybody could really hurt us." And then showing them yep, they really could. There's a bit of a religious conversion that happens there. And once those people are converted, they become some of the best advocates for then following through to the very end. And the descriptions of Ukrainian incidents Sarah gave also, I bet somewhere in the audience viewing this conversation, there's somebody who's a pretty advanced technical thinker. They know the way grids work, the way transformers work. And they're a little bit unsatisfied that – I wish these guys could have been a little bit more technical. They really watered it down too much.

I invite you, and it sounds like promotion. It is a little bit, but I'll keep it moderate. If you go to the appendix of the *Countering Cyber Sabotage* book on CCE, there's a case study on a fictional, Central to Eastern European country called Baltavia. I just want to say right up front, it's Baltavia. It's not Ukraine. It's completely not Ukraine. But it should satisfy the most ardent technical person. It should scratch those itches. It's almost unreadable by anyone else, but for certain people, it really communicates how CCE works against these top tier threats, in exquisite detail.

RAVICH: I want to get back – Oh yeah, please, Andrew.

HILDICK-SMITH: Yeah. Just adding on to Sarah and Andy, as Sarah was saying, the Ukraine attack had some basic elements, and the things we're seeing in the water sector are super basic. It's just remote access. And so, lots of utilities are vulnerable. And one thing that every utility can do that's really useful, is to think through the manual steps for their operation. And they may not be able to completely do the whole process. The pressurization and the treatment. You may not be able to do everything, but if you can at least do the pressurization, so that firefighting can happen, work that out. And then take the time because there'll be ways to adjust your process.

And it may take some effort, but eventually you can come up with a way to, in quotes, "manually," because you may have separate control elements, that are independent, that help you run your system. If your SCADA system's breached, you want to turn that off, and disconnect and run manually. And so, that re-utility can think through that with those in-house experts.

And in this case, they'll need some help from some process control people to think through it. But that's important. And then just one last thing was, in 2018, I think, Andy published a piece in the *Harvard Business Review*. Which was really helpful for us, because it got our executive office attention, because it was the right language and it made it clear that what we were doing was not off the wall stuff. It just made sense. And out of that article, we then went back to look for other issues. And the first part of that process was bringing in the maintenance, the engineers, everybody who had a stake in the process working. Regulatory, every aspect.

And then it was a case of, forget that we have any security, just assume that a bad guy can do anything they want. Don't limit yourself. Just imagine the worst things, the things that you worry about at night, just happen. And then we can come up with that list, and then try to come up with ways to protect your system. And we're used to calling it cyber physical safety systems. So, as a safety system, other groups of people can appreciate that, and think, oh yeah, that makes sense. Maybe we're not protecting – Or maybe we're protecting the customers, but sort of, first we're protecting the process and the equipment.

BOCHMAN: I just want to say, when – pardon the interruption, Samantha. But when you were describing figuring out how you can run less optimally, but still keep things going with manual and semi-manual modes, we have to play another day, is a beautiful textbook description of resilience. The ability to operate through. And I know the Cyberspace Solarium Commission advocates for this. And it's just the best way to think when we're dealing with these topics, which can seem overwhelming.

RAVICH: That's right. We did take it on in a Solarium as one of the key planks in deterrence. If the adversary knows that you can actually fight another day, that you are not going to be down for the count and completely out of the game after an attack, it gives them pause. That they won't be able to reach their goals by some type of massive attack. I want to get back to this conversation about the human, in or out of the loop. And so, Sarah, one part of CCE that I really do find interesting is, is of course the idea that this – Keeping a human out of the loop actually has significant downsides.

And across industry, there's an increasing embrace of automation and remote connection, as a cost savings mechanism. In our own CCTI discussions with small water utilities, that's the way they say we have to survive. We don't have many resources. We have to get this reasonably cheap, whatever price, widget, and fire lots of people instead. And companies also, they tout the efficiency of all digital systems and the removal, as if, the removal of all human error. But CCE takes a different approach. So, walk us through this.

FREEMAN: Of course. Yeah. CCE does recognize that in some cases there's reasons why market or otherwise – There's been constraints on the environment. Organizations have adopted automation. We're kind of neutral on the topic. I think that that's where the market has gone. And I don't think we're going to get rid of that, but there is value in having a human in the loop. We talk a lot about examples, specific examples, where the human is sitting there in front of the screen, like in the Oldsmar case, there's other incidences that have that kind of option.

But sometimes, the human in the loop is – It could be someone that's not sitting there in real time. So, depending on how you insert that perspective. What we're really getting at, though, is perhaps, maybe we shouldn't make our digitized systems all-powerful. So, there is a limit to advantage there. Obviously, you want to get all your financial returns, in terms of automation and control. And in some cases, it may make sense to automate. But there are physical stop gaps that can be put in place in case there is manipulation or loss of control of the digitized system. That's something that I think – It's been around for a few years. A lot of people, especially in the Beltway area are familiar with Richard Danzig's *Surviving on a Diet of Poisoned Fruit*. But it's that concept of engineering in resiliency, more than engineering out humans.

So, you might want to engineer a human in, back into the loop, if that's your resiliency plan. But the other part of it is, is recognizing that there, just like the human, and there may be an insider threat. They may be the savior. Just like that, your digitized system may also be both a threat and a help to you. So, recognizing that's a neutral concept, it could be used either way for good or for evil. Maybe we should constrain what the full power and capability of those systems are.

RAVICH: Oh, Andrew?

HILDICK-SMITH: I mean, one way to look at it maybe is, the digitized system's really important for all sorts of industries. But you can design it or customize it after it's already in place, in a way that the critical components, and that might be your control elements, the pumps, or whatever's at the end – Or a skid-mounted process, or in water, it might be UV, or ozone or something. You can wire that in, in a way that it's not on your network. You can have four to 20 million connections. So, it's not a smart communication. It's just passing data that you can't – You can manipulate it. But it's something that you can't attack in a traditional way, and so you can save those components for when your SCADA system goes down, and your manual or semi-manual process. You're protecting that equipment along the way, even though it's a control system, automated, but you can hybridize it to preserve really important parts of it.

RAVICH: Great. Andy, I want to get to, I think, one of the most telling, or most colorful or most impactful examples in the book, about the importance of keeping a human in the loop. And you call out Stanislav Petrov, the Soviet Lieutenant Colonel, who, as you say, may have saved the world in 1983. So, tell us a little bit about that story, as well as how that actually made you think about incorporating some of the principles from that in CCE.

BOCHMAN: Sure, sure. Thanks, Samantha. Yeah. For those of you who don't know it, if you were born after 1983, you almost were never born. And if you were alive at that time, you would have had a very bad evening. Around midnight,

in the Soviet, then Soviet Union, equivalent of NORAD, they just stood up a very complex computerized system to track inbound ICBM's. And Stanislav Petrov, a Lieutenant Commander, not the highest ranking person in the control room by any means, but the chief architect of the system was on station that night when all of a sudden everything went off. Just picture sirens, klaxons, lights flashing. Ultimate red alert like on Star Trek.

And their job – First, they did a query to the system, because there was a way to sort of gauge the degree of confidence. And the system came back and said, high – Highest confidence. This is for real. That just made the humans – Again, the human element, right? That just made the humans, just, even more frantic, and nervous. And they were on the verge of calling the Kremlin. Calling the government leadership and saying, we need authorization to launch all of our missiles at the United States. And so, Petrov was there though, and he knew this was not a perfect system, as there is no perfect system. But he really knew that, in a way nobody else in the room did.

And he pleaded to the higher ranking people there to, please, let's wait until we get some corroborating or orthogonal – Other data from our other sensors, other humans, around the world, before we go call the Kremlin. And they did wait. And the other folks chimed in from around the world and said, "We don't see anything. It's nothing. Nothing's going on from here." And then, everybody could breathe again. And exhale. And bring the system down. And they did forensics later on and figured out what had happened.

But you have to understand that if that particular person, I think in the book we call him the "ultimate man in the loop," hadn't been there, they would have launched. And then we would have launched. And then it would all be over. Now, that's about as dramatic as you can possibly get. And you might be saying, well, our business isn't about the end of the world. We're just an international cheese manufacturing company, for example. Still, if that's your livelihood, if that's how you make your own living, and your employees and your customers are loyal to you, it is kind of the end of your world if that all goes crumbling, all of it goes tumbling down.

So, when Sarah was remarking on it, and others, sometimes for some things, it is worth it to pay a salary of a person. A person you trust, who has knowledge. And they don't always have to be in the room, but to be parts of the most critical parts of the process, to have an eye on those things. You can imagine that could pay for that salary many times over.

And just a quick footnote. If I was writing, it would be a footnote. The documentary on Lieutenant Commander Stanislav Petrov is called *The Man Who Saved the World*. And so, you can find it if you want to check it out. I recommend it.

RAVICH: That's fantastic.

BOCHMAN: He did. He really did.

RAVICH: Yeah. That is fantastic. I know what I'll be watching tonight. I mean, Andrew, or to any, maybe a last question before we get into policy recommendations for a few minutes. So, FDD, CCTI, alongside of Idaho National Lab, sponsored by the Department of Energy, created an Operational Technology Defenders Fellowship. And Andrew, you have talked about the unique challenges that OT professionals face when their systems are, maybe, being replaced every decade or so, where the IT professionals, a new system is coming along much more rapidly. And again, we're speaking to a broad policy community on this panel, talking to folks on the Hill. What do they need to know about, not just the

differences between OT and IT, but the unique challenges that the OT workforce is facing along what we're talking about today? The shape of the battle space.

HILDICK-SMITH: So, yeah, like you were saying, it's a timeframe issue of, so you have your treatment plant or your pump station. It's set up with programmable logic controllers and they're programmed and they're in place, and they're very reliable pieces of equipment so you don't want to mess with them if you don't have to, and they go out of their life cycle over decades, two decades, or it's a long period of time before the companies stop supporting that equipment, and so you're often not forced to spend what can be millions of dollars to upgrade for long stretches of time.

And so that's part of why CCE is really valuable, particularly the engineering, the system for resilience because it's providing the protection that you might not be able to incorporate in the network part of your control system because the equipment's aging and you're not able to replace it easily. So, having safety systems or engineered controls or the manual operation plan for those fallbacks, it becomes much more important for versus the enterprise where maybe every five years, they get a complete replacement of hardware and software.

RAVICH: Let's turn to broad policy recommendations or how we get the concepts of CCE to a broader base of people that need to know and understand this. So, Andy let me start with you.

BOCHMAN: Sure. A couple of years ago, a first step was made in this direction. It was before the dawn of the Cyberspace Solarium Commission, but it was Senator Angus King, the eventual co-chair of said Commission, and in my opinion, one of the smartest people on cyber topics up on the Hill. He in conjunction with Senator Risch of Idaho, advocated for, it took a while, a piece of legislation called the Securing Energy Infrastructure Act, and it said things that sort of got the press a little bit riled up. One of the terms I know they focused on was "the selective reintroduction of analog technology." What? That's heresy. We believe in progress, not going back to the stone age. This bill would dumb down the smart grid. I'm not anti-press. That was one way you could interpret it, but that wasn't the intent of it and that's not really what it's about.

It's about things like considering putting a person back in the loop, it's about fail safe and stop gaps of a mechanical or physics-based nature to save the day when it really gets that intense. So, I'd say to me, that was the first shot on the policy side that ties tightly into this, and then again, the work of the Solarium Commission in, I think there are 80 in the initial publication, plus or minus, and a number of them speak to this, especially every time we get to resilience, anywhere in that vicinity, or continuity of the economy, continuity of missions. We're talking about things, protecting things that must not be allowed to fail, and if they do fail, then having a plan B and a plan C so that you can keep operating through.

So, that's, I think the commission has picked up the torch from Senator Angus King and Senator Risch and is carrying it through. A lot of what you could do in the future would be, and I think, again, these are in the recommendations, educating people, educating folks that live on the front lines of these most important, critical infrastructure systems on some of these approaches. It doesn't have to be CCE exactly. Just to let them know that there's an alternative to business as usual, and again, I'm not anti-RSA conference or any vendor, but if that's all we have, we're going to end up staying in this extremely uncertain position, which is very uncomfortable for the foreseeable future. We do have, I think, a way out of that at our disposal now.

RAVICH: Thank you. Thank you. And Solarium, we have been empowered for another year, so we are going to be keep pushing these critical and important issues. Andrew, maybe some thoughts on what the folks in Washington should be focused on?

HILDICK-SMITH: Yeah, I would say for the water industry, if you can – I don't know if requires is the right word, but it would be really excellent if every water utility had that manual fall back plan to whatever level they can achieve, but that it's documented and practiced. So, you can maintain whatever level of service because you, like what Andy was saying, right now, there's not a way to protect yourself in the cyber world and so you need that fallback, that resilience. So, that would be it, and take advantage of the staff, the engineers, the maintenance people to come up with those protective measures that can kick in if either by an operator error or a cyber adversary attacking and trying to cause mischief. So, those are two things.

Thank you, Andrew. Sarah, I think I'll give you the last word on policy reflections, but also other things that we may have missed in this discussion.

FREEMAN: Thank you. I don't often get the last word, but there we go. I think one of the key things to keep in mind, we talked about this a little bit, but we didn't clearly state it. I do a lot of work focused on threat capabilities, threat vector growth, but I think we tend to look at that in a vacuum and not recognize the other actions that are going on. If we look on the other side, on the defender side, there's market forces, there's other things that are happening that I think policy can be directed against. At Idaho National Laboratory, we usually call these out as increased digitization, which we have talked a lot about, but also increased integration. Those two go hand in hand.

The fact that there is actually a shrinking market space in many critical infrastructure sectors so there's a small group of vendors from a targeting standpoint, from the adversary's perspective, that makes it a lot easier to develop capabilities. And then ultimately, we do have a lot of engineers who learned a different type of engineering in some ways, and they're retiring, and they're retiring in part because we replaced some of them with automated systems, but those pieces should probably each be addressed in their own ways. One of the things that comes to mind, for example, especially given INL's nuclear background, we talk a lot. That's very much a shrinking industry. It's really hard to teach a nuclear engineer the same way that perhaps we taught them decades ago because they're not necessarily in a position to build new nuclear power plants and new control systems from scratch.

And that's something that as a policy, I think it's really important to push for that innovation. We talk a lot about educating the workforce and that's important, but I think the key part of that education is actually allowing room for some of that innovation and that's going to require a lot of, I guess, some investment, but also the willingness to allow people to experiment and try new things. On the shrinking of the market space, obviously that's a lot more complicated of an issue. It's globalized economy in terms of the digital goods, in terms of where we come from, where our stuff comes from. You've heard a lot about it, knowing thyself lately, especially with things like software bill of materials, hardware bill of materials. That's a great place to start. I think that the reality is we've probably gone really far down that path where it's really difficult at this point to start producing a lot of those materials inside the United States.

So, from an engineering standpoint, what we want to encourage is that people recognize that diet of the poison fruit concept again, and we start developing mechanisms that allow these systems to operate, even if sub-components within them are potentially compromised from a supply chain standpoint. And then finally, if there is a preference for specific market vendors, the market economy on the world stage is complicated by a certain degree of subsidization that

goes into for certain vendors. So, if we do want a preference for particular companies, particular technologies, we may have to consider subsidizing those particular technological solutions.

RAVICH: Thank you. I want to thank all three of you. This was a fantastic session and I actually can't wait to listen to it again because when you're moderating, you're moderating. You're not always able to focus on all of the really fantastic recommendations that came out of this panel, and as we had talked about, it's often times a very dark discussion, but in a way, I felt this conversation was comforting because there is a process that we can follow and learn from to help our resilience, help our country's resilience. So, on this Friday, it leaves us hopeful. Again, thank you. I can't thank you enough, and for those of you listening who haven't yet read the book, I highly recommended it. I'm not sure who's going to play Andy and Sarah in the movie version but stay tuned. We'll get to that at a different point, but again, thank you. Thank you very much.

BOCHMAN: Thank you, Samantha. Thanks everybody.