Eric Hess: [00:00:00] Hi, this is Eric Hess of the Encrypted Economy. Over the last 10 years or so we have focused so much on securing centralized systems, particularly the cloud. But our dependencies for security extend fully to the edges of our networks through IOT, mobile apps.... as our dependency on these edges increase, so do our vulnerabilities. As our digital, and sometimes encrypted economy faces growing threats from state sponsored actors, and just highly sophisticated cybersecurity attackers we have an awful lot of threat data to model across more devices. Machine learning threat modeling requires a lot of data and time.

In some cases, it works well. Other cases, maybe not so much. On today's show, we explore the Koopman operator methodology with Igor Mezic, the CTO and chief scientist for mixmode.ai. It's a cybersecurity threat modeling platform powered by what they call unsupervised AI. The Koopman operator methodology of artificial intelligence provides an alternative or supplement to current data and resource intensive threat modeling, as well as other applications. For example, in addition to cybersecurity, Igor also has focused on smart cities and a lot of other applications for the Koopman operator, but it's easy to see how cybersecurity and smart cities go hand in hand. Like let's take a recent example. Oldsmar Florida. It's a city of roughly 14,000. Sits right between Tampa and the sunny beaches of the Gulf coast. They have IOT systems that discharge chemicals into the water supply there to control water potability. One of these chemicals. Is sodium hydroxide. It limits pipe corrosion, removes heavy metals from the water, and manages the acidity of the water. It's also the main ingredient used in drain cleaner.

This chemical was adjusted from 100 parts per million to 11,100 parts per million in the water supply by a hacker. At such a high level, it is considered highly corrosive to any human tissue it touches. It was stopped, but it's concerning. And there are a growing number of incidents like this. Both in the U S and abroad.

In Australia, remote access enabled millions of gallons of raw sewage to be dumped into local parks and rivers. In Ukraine, open circuit breakers remotely turned off the power to a quarter million people.

I haven't even touched on ransomware attacks. Question, is a resource intensive machine learning threat detection model up for challenges like this? Even putting cybersecurity aside. Everybody knows that current machine learning is not self-executing. As Igor states in this episode, machine learning is not really learning at all.

So in this episode, we consider how the Koopman operator methodology adds the dimensionality of time to make it a less resource intensive, and depending on the use case, more rigorous alternative to current machine learning methodologies. I hope you enjoy this episode as much as I did. If you like it, share it. If you have comments, reach out. And now for our episode with Igor Mezic.

This is Eric Hess with the Encrypted Economy and I'm really excited to have Igor Mezic, a professor at the university of Cal Santa Barbara and the chief scientist at mixmode.ai on the show today. He has quite the background with regards to artificial intelligence, but even more importantly, he comes at it from a very different angle, which they apply into mixmode as a cybersecurity service. Before I continue, Igor, do you want to give a little bit of your background for the listeners?

Igor Mezic: [00:03:55] Sounds good. So I have straddled the fields of mathematics and engineering quite a bit in my career. I did my PhD at Caltech in what is called applied mechanics and then did a post doctoral fellowship at university of Warwick in the UK. And there I was at a mathematics Institute. But then I came back to engineering and joined the college of engineering at the university of California Santa Barbara, and there I also belong to the center for control dynamical systems and computations, so I run the lab. And then I have quite a bit of interest in entrepreneurial activities and currently I'm the chief scientist of Mixmode. We are deploying some of the artificial intelligence methods that we develop the algorithms for in network security in that context. But also at a larger scale there's consulting and software development company called AimDyn that my wife and I founded back in 2003, that does designer AI type things. So AI for specific service problems.

Eric Hess: [00:04:55] So Igor is a well-known in the AI space, particularly with regards to dynamical systems. And his name is synonymous at this point with the Koopman operator which he has done an enormous amount of work with. In fact, he is going to be a recipient this year.... I don't know if I have permission to do this but I'm doing it anyway, the recipient of the JD Crawford prize, which is a biannual award presented by the society industrial and applied mathematics for his work in the field of dynamical systems, which is quite the prestigious award. So congratulations on that. So before we even delve into it, I like to ask my guests about a single experience that shaped your values, your worldview, or your career path.

Igor Mezic: [00:05:37] I was in high school, I think. And I found this article... I was reading this journal, popular science journal, and it talked about chaos theory and how exciting the world of dynamical systems and chaos theory is.

And they were talking about these various dynamical processes that are complex, but yet at the same time applied like the water coming out of the faucet is turbulent and chaos theory can explain that. We can talk about whether chaos theory got all the way there. Not really, but it was very exciting. And I think my love for science in general was really prompted by reading that article. I think I was primed already, but I decided to make my career in dynamical systems and to start with chaos theory, really. And then later these algorithmic approaches like machine learning and AI.

Eric Hess: [00:06:27] When Igor and I were talking before the show I had done some reading and learned a little bit about jet engines and the application of dynamical systems to jet engines and Igor says, "I worked on that", of course, I think Igor worked on everything. He's across the board, but what was the first project, the big project that you worked on with dynamical systems after you graduated?

Igor Mezic: [00:06:49] That's a great question. I, consider that one as a kind of a career forming project. So a friend of mine, Andre Barashut was at UC Davis at the time. And there was a big project going on and it was led at UCSB by Peter Cottilege. And it was on controlling jet engines. And so Andre went to United technologies research center and asked me, Hey, do you have an idea of what would be a good methodology to do some diagnostics on jet engines so that we can figure out whether instability has happened very early on in the design process when we have those a jet engines as just small versions on

a tabletop. Combustion chambers, let's say on tabletop. And the problem was very severe because of course instabilities in a jet engine, they can cause very serious problems during flight. It's very costly to build a full-scale jet engine.

Eric Hess: [00:07:41] Yup

Igor Mezic: [00:07:41] So if you could do something on a tabletop, it's a good thing. So I designed an algorithm from a perspective of what's called ergodic theory. It was really Koopman operator theory in one particular context and domain. And I was finding what I think we're going to discuss a little bit is eigen function as in eigenvalues of an operator. It was very abstract, but at the same time, the algorithm worked like a charm. And I think... they tell me that I think even today, they run these tests with that particular, let's call it AI algorithm to do diagnostics as to whether, small scale model was going to translate to the large-scale model and whether it is going to have any instability or not. And so the reason why I think that was a very important moment is that I realized that this abstract stuff on the operator side actually has a very practical edge. And that is because instead of the usual starting point in dynamical systems when you need a model, you need a set of differential equations or something to work. Here I could do everything from data. It was entirely what they call data driven. And this was 1996 to 98. So before data-driven was a thing. We certainly did extract properties of dynamical systems in a very complex one with single pressure probe inside the combustion chamber. We were able to predict whether the instabilities were going to happen in that engine or not.

Eric Hess: [00:08:59] And you'd certainly think that's where you'd be able to get experience with dynamical systems inside a jet engine. In one of your more recent papers, October 2020, you state we're in the middle of a sensing revolution, where sensing is being used in the broadest meaning of data acquisition. Most of this data goes un-processed, un-analyzed, and consequently unused. This causes missed opportunities in the domains of vast societal importance, health, commerce, technology, security, just to mention some. Do you want to expand on what you're writing about there?

Igor Mezic: [00:09:34] Yeah so, we now measure everything right? The metrics are put on everything. The metrics are put on scientists outputs. But the great question in information theory is not... we know what information is for a long time from Shannon, right? We know how this guy was mathematically. There's another concept that I always think about, which is useful information. And if you just think about the human brain, it also measures a lot of things. It gets acoustic signals, it gets visual signals, it gets tactile. And then most of it, it just dismisses. It's not very important it's standard stuff. And then there's some stuff that we react to , or we like to be engaged with the process, right? And that's where our brain sort of picks up the feedback from measurements and then interacts to in sports and a variety of other things. So artificial intelligence is in some sense, no different if you apply it to the issue of sensing that we are doing across these different technologies that I have mentioned, but there is a... so it's not different in its purpose. It's supposed to take the data, the raw data and extract useful information out of it. That's really what should happen with well-designed algorithms of the sort. But it's really not a copy of the brain because the types of information that's coming out is in general different.

Network data is something that our own brain has to spend a lot of time learning how to understand and analyze and coarse grain and we are very good at this. The network security analysts that are really good at this, how do you get then artificial intelligence so that to do that, to extract that information that is really useful is really the point of that remark. So we should be throwing away most of the data, but not all of it. Maybe we should be aggregating it into larger concepts that then can be presented in the interaction with the human. Here is an important points, I'm not thinking of AI as a self governing, taking over the world or something like that. I'm thinking of it as a helpful tool for humans. And so the last step in that is okay, you've extracted some useful information to me that you, the AI think it is. Why don't you present it to me in the terms that I can actually understand?

Eric Hess: [00:11:45] And so we also talked a bit about, and this sort of, I think, connects to another point that we discussed, which is machine learning and the approach of machine learning versus the dynamical systems models that you work within the Koopman operator. Do you want to speak about that a little bit, and the limitations of the machine learning model versus the dynamical systems and the koopman operator.

Igor Mezic: [00:12:10] So I'll be a little controversial here...

Eric Hess: [00:12:13] Be controversial!

We love it on this podcast.

Igor Mezic: [00:12:15] I actually don't like the use of the term learning in those contexts, machine learning. To me, those kinds of methodologies are great functional approximation methodologies in mathematics, but I would reserve learning for this process that I've started describing in a previous answer, which is, learning for a kid is really forming a set of patterns and meanings to patterns that can also interact with each other by a process of acquiring data, forming a coarse grain pattern recognition ability, and then having the parents every now and then tell them, that's a cat. Or the child goes, well that's a cat... no, that's a tiger. You should stay away from that. That's learning. Learning is not giving a kid a bunch of inputs and photos and then having them recognize something else as that. It's just, I think a misnomer. There is a misnomer between the mathematical usage of the word learning, which to me is functional approximation and, deep learning methodologies are fantastic at that. So I think of learning in slightly different terms. And if you notice my perspective on learning has time embedded in it. So you acquire the data and then something interesting shows up and maybe you form an internal label for it if there is nobody around. But if there was somebody around, you might either ask, or somebody just can say, that's a cat. And at that point in time, you formulate that correlation and you move on, right? Oh, that's a dog. And you're not given a massive amount of information at the same time. And so this is how we build the ability of finding causality. I know it fails from time to time, many times it fails and what can come out of failed causality is a big issue, but humans are actually very good at causality. And functional approximation isn't. The relationship between the data inputs and outputs, doesn't say anything about whether anything on the output is caused by anything on the input. So my perspective is that you don't have learning without a specific treatment of time and you don't have causality

without specific treatment of time. And that's what I pursue really. That's my research program, right? To embed both of these into AI.

Eric Hess: [00:14:39] And the time component of the function is a variable in the equation. That is part of the underlying algorithm, if you would for this dynamic modeling.

Igor Mezic: [00:14:50] Yeah. And if we live in the Newtonian context, then it's an independent variable, meaning that outputs and inputs depend on it. So at any given time we have a set of inputs and the set of outputs and of course time evolves, but it informs all these other ways. So yeah, it is an additional variable that I think cannot be put in artificially.... just pasting it on, but has to be treated for what it is.

Eric Hess: [00:15:16] You're the star of this show, but your CoStar is the Koopman operator. So do you want to give us a little description of the Koopman operator? Because it's impossible to look up Igor without finding the Koopman operator? It's an area he's been focused on as we've been discussing, but let's start to try to put some definition around what it is and how it operates.

Igor Mezic: [00:15:35] Okay, I'm going to start with the fact that about a hundred years ago, there was a huge revolution in science where quantum theory was discovered, and the idea was that people were measuring these various spectral components in atomic processes, and you couldn't really observe the positions and the loss and the momentum of these atoms, but you could talk about observables that are the spectral components. And so Heisenberg said I need a theory that's going to tell me about those spectral components. I can't totally measure positions and velocities and he developed a theory that is structurally very much what is called an operator theoretic perspective on that process. He basically says you know, what I'm observing is really not a mathematical function, it's an operator. It's really something more abstract. So Koopman understood this and said, Hey, if I have a classical mechanics problem and he worked on these classical Newtonian aspects... couldn't I do the same thing? And he said here is an operator that could potentially do that. It could take a state of the system at time T to the state of the system at time T plus Delta T sometimes later. You can think of it as a big matrix that just takes the state of the system at time T and ports it to some later time. Now, that sounds more complicated than Hey, mass times acceleration is equal to force, but it really isn't and it's more powerful because acceleration is the second derivative of position and a position is the state that somebody told you, you should worry about the state, right? The position. If you think about it for a second, what is the most used physical term in this universe? Energy. It hasn't anything to do with the state it's actually composed of the observable, that's a momentum and an observable that is a potential, which is a functional of States. So it's not the state. It's some observation on the state that we call energy, and we have TV programs on it all the time because it's very important to us. The point that I'm trying to make is if somebody gives you data, they might not give you the data in the best possible format. Figuring out the position is a great thing if you're designing an airline path from LA to New York. But you're actually, if you're United airlines, you're more interested in how much energy that airline is going to spend, because that actually affects your bottom line.

So that was the original thought that Koopman had. Why don't we design something very similar to what Heisenberg has said in quantum mechanics? And I'll deal with the variables

that are either available or important. And so he designed a formalism that is this operator theoretic form that takes concepts like energy from one time to another via operator means. And then von Neumann famously picked up on this, von Neumann is much more, I think in general terms much more famous than Bernard Koopman who was a mathematician at Columbia. And then they worked together, and then that particular theory was put aside for a while because, it was just a little bit in physics, but quantum theory dominated and they didn't go back to quantum theory... understanding quantum theory from this perspective. .

So I started thinking about this during my PhD thesis and I found a good use for it because we were interested in understanding mixing and fluid flows. And sometimes in mixing, you have domains that don't mix very well. This could be either good or bad, if you want the good mixture of various things, then that is bad. If you don't want a certain pollutant to cross across a certain boundary then it's obviously, mixing would be a bad thing and existence of separate domains would be a good thing. So I used it to visualize those domains because I could find observables that could separate these components where I said Oh, this is useful, but it wasn't developed for things like jet engines because that is dissipation and crazy stuff like turbulence going on and things like that. So then a jet engine story comes into the picture and I started thinking, Oh this is really useful. And then I focused all my efforts on systems with high dimension because I figured out it works in jet engines.

The jet engine dynamics is very high dimensional. So that's a little bit of the history how, Koopman came to the idea of the operator. And then how that became useful in a data driven context that's obviously Koopman didn't think about because it was not a thing.

Eric Hess: [00:20:01] So basically you're the one who took Koopman out of the closet and dusted it off. It was still out there, but it looks like a it's certainly being applied more since your engagement on it.

Igor Mezic: [00:20:10] There are people that pay attention, especially mathematicians in robotic theory use it quite a bit from the perspective of pure mathematics. There are also people in physics that are using it in a variety of different contexts. But okay, if I have to take the credit, I think the aspects of data-driven that I think I understood pretty early is a potential and the connection with things like learning and, modeling dynamical systems processes, I don't think that was very well understood even for myself before 2004, 2005, really. I guess that's the progression. And then, with many collaborators and students and postdocs and people from all over the world literally, then we collectively push this to be what it is today, which proves itself to be pretty useful in a variety of contexts.

Eric Hess: [00:21:06] It provides a very rigorous method for linearising the system dynamics. Is that correct?

Igor Mezic: [00:21:14] So I would say that's how it's used today in a large majority of cases. So remember when I said position and momentum, right? And then you have energy . Energy is actually a square of momentum plus the squaring position. It's the energy for a system that doesn't have friction, doesn't change. So the idea here is that you

can find variables in which the system looks linear. And if the system looks linear, I think in physics, they would call it the change of gauge. You just basically find some other variables in which the system looks linear. And the key concept here is that you want to make it finite, dimensional, and linear. Then it's really useful.

Eric Hess: [00:22:00] If it's not linear and if it's not finite, then it's more theoretical.

Igor Mezic: [00:22:04] Yeah, yeah, yeah, you cannot really get any applications. But in the 2020 paper, what I proposed is that it's quite useful to look also at what they call the finite dimensional non-linear representations of the Koopman operator. And that goes exactly along what you've just said. Which is, you can always say that there is a representation of aero-dynamics with the Koopman operator, but it is infinite dimensional. So if you don't have what is called Eigen functions, you cannot reduce that to a linear, finite dimensional presentation.

So there's a whole class of systems for which you can, and there are complex systems in which you can't. So I turned it in this last bit, but I turned it a little bit on its head and basically said, look, how about I look for finite dimensional but nonlinear representations of the operator. And that's going to enable me to compute some really nice things. Now I'm not going to have a linear representation. These are systems like Lorenz system, the famous chaos theoretic. You're not going to have a finite dimensional linear representation probably. And that's a nice thing about Koopman operator theory. You can actually prove things. So you could prove that it doesn't have a finite dimensional linear representation, but it has a really simple finite dimensional nonlinear that representation. And in some sense, that's a concept... this has been known for, obviously for a long time, but it's in some sense a consequence of this Koopman theoretic point of view. And so I'm hoping there's going to be a lot more of that where you start realizing okay, maybe I can get through this mechanism of finite dimensional nonlinear representation. I think people are working on this around the world as we speak.

Eric Hess: [00:23:41] So we've gone theoretical a bit. Hopefully the listeners have hung on. I'm like , I could probably extend this probably longer than most people want to listen to it but don't take that the wrong way.

Igor Mezic: [00:23:53] No, absolutely not, I hope it was at some level understandable. But to your point, give a simplicity in understanding of the systems is what we are really going after. And whether at the end it's linear, which in some cases is, and that's beautiful and very helpful. That is great. In some cases it could be nonlinear and still very useful.

Eric Hess: [00:24:15] Let's just talk about each of those. We're not going to delve as much into the definitions cause we handled a lot and you talked about finite non-linear and we talked about finite linear application. Give me examples of the use cases for each.

Igor Mezic: [00:24:29] Okay. So if you're working in the context of control theory and say you want to stabilize the temperature in the room to a certain, very specific temperature. Usually that's done using feedback control. So you measure the temperature, you apply some controller, maybe it has aspects of being proportional to the difference between the temperature you want and a temperature you have. And you go to that finite fixed temperature at the end. Such a system, even if the approach to that equilibrium, to the

temperature that you want is not linear, it typically has a Koopman linear representation. You can find, let's say n eigen functions and when you write down the equations for those eigen functions, they actually give you a linear system.

So you can treat stability problems exactly using this kind of an idea very nicely in this context. So that's the context in which you have a linear representation and in the Koopman world we say that this is driven by the fact that the spectrum of the operator. So you can think of a spectrum in the same sense you think about it in the classical context, like you have a certain repeated frequency and that's a spectrum.

The only difference in the Koopman world is you could have also exponentially decaying or growing things. And the rate at which you're exponentially decaying or growing is also a part of the spectrum. So it's not just the frequency like the classical transfer, things like that. It's also the growing and decaying processes. That's why we can capture a recent aspects of COVID explosions, exponential explosions, because the growth rates are exactly the Koopman eigenvalues. That might be an interesting side topic, but let me go back to the question that you ask, which is in which cases do have a finite representation.

If you have in your spectrum, just eigenvalues, so just these growing decaying rates and oscillation rates, then you will have a finite dimensional linear system. If you have what is called continuous spectrum, meaning let's say your frequencies are continuos with distributed. There is no one single frequency that your signal has.

It changes all the time. For example, the output of the Lorenz. If you just monitor the X variable in the Lorenz butterfly, it's constantly going to change in frequency. You think you caught it for a while, but it oscilates at a certain frequency and then it changes. It goes to the other wing and it goes back and goes back. Those are the systems that don't have finite dimensional linear representations. For Lorenz we know the finite dimensional nonlinear representations, but there are many systems out there, like from which you can extract this finite dimensional nonlinear representation from data. That's the idea.

Eric Hess: [00:27:13] So going back to your paper where, you specifically referenced the opportunities in health, commerce, security, let's talk about how the coop and operator could be used in the context of each of these.

Igor Mezic: [00:27:25] Sounds good. Let's talk about health. We are now measuring fitness of a lot of people around the world. And the basic measurements are those of the heart rate and so on and so forth. I swim on literally a daily basis with my iWatch and I can see how poor my performance is. And of course we are throwing away most of the data coming back to that topic from earlier. But for example, using this operator technique, you can essentially build personalized models, just let's say for blood pressure and heart rate variability, and we have done some of that. There's a paper in the American journal of physiology with with my collaborators, where we have essentially structured the model by using techniques that are based on the Koopman operator ideas. And the feeling was that we could utilize those models in personalized medicine. For example, if a doctor would know the elasticity of a person's blood vessels, that would help quite a bit in dosing the medication for any kind of heart disease or generally cardiovascular disease. And that is a hard thing because you don't open someone up just to figure out what the elasticity of their blood vessels is right? So these methodologies actually enable you from data to

figure out parameters like blood vessel elasticities without opening up anybody. So to give you a simple reason, why is that, for example if I throw a ball and it falls somewhere and I want to deduce the velocity with which I threw it, I don't need to measure it. The only thing that I need to know is really the distance that it went, because I actually know what, the gravitational constant is. So I can infer the velocity as long as I had some data on how it went.

Eric Hess: [00:29:18] So a practical application of that would be for example, if somebody has like a heart arrhythmia so your doctor will say, please wear this Holter monitor for a week or two weeks so we can collect data, and then we know if you have an arrhythmia that's very basic. Would that be the way that it would be used or would it be more like something that you would wear, like your iWatch and it would detect something else and over time it would be able to understand the elasticity.

Igor Mezic: [00:29:41] Yeah, I would say both. And just for thee record this hasn't been used in this context yet. People do a lot of signal processing kind of techniques for this purpose. There is a lot of work out there on processing the data on heart arrhythmias and things like that so I'm really not claiming that there is anything that we contributed to that particular area just to be clear, but the potential use, right? Because there are many facets of the operator itself or a large amount of information that is in there that can be connected to the health aspects, so both. Let's suppose that I can do this offline in the doctor's office and somebody measures the blood pressure and the heart rate variability, for example. And I can use the Koopman operator theory to find the elasticity of blood vessels at time T and then let them wear a watch. And then at time, T plus Delta T, I do the processing again. And I find out there is a serious change. That's something that could be sent back to the physician. So it's the methodology that can be used in both contexts.

Eric Hess: [00:30:46] That's a good example. You mentioned COVID before, so before we jump off of health let's talk about how in a pandemic setting, obviously a lot of data out there, how might the Koopman operator facilitate efficiencies in how we treat, vaccinate, assess the rate transmission.

Igor Mezic: [00:31:02] Yeah and this is some early work with Aimdyn that I mentioned before, and also, was supported by DARPA. So when the pandemic started, we got the data feed from Johns Hopkins. And as to the question, whether you could predict the evolution over short timescales so that perhaps the occupancy, you know... hospital bed occupancy can be adapted based on that information. And the reason why this is a really nice methodology in the context of a pandemic is that there are these exponential growths. As I mentioned earlier, the exponential growth is encoded in the eigenvalues of the operator. So we had some really nice early success there. And then we ported that into thinking about how do we design logistics based on that? If you're seeing and predicting the next week or so, there's going to be an outbreak, the logistics of, for example, hospital beds, is Important. And also you can plan, and this is some research that they're planning on doing right now planned the vaccination procedures as well, based on this particular information to get the vaccinations to the places where they're more needed in a short amount of time.

Eric Hess: [00:32:15] Okay. Now shifting gears to commerce. Commerce is broad but what are your thoughts there, in terms of the use of the Koopman operator? Is it a logistics component? Is that what you were contemplating?

Igor Mezic: [00:32:26] In the context of commerce, it can certainly be used in the context of logistics. And that's something that we wrote about already. There are papers out there that even study the stock market evolution from this perspective and that's not us. It's actually a couple of different groups around the world, but as it being, the data processing technique that is pretty general, I think you see that you could monitor and model the evolution of stockpiles of a certain product in the marketplace and do predictions or understand how to control the flow of supply chain, and so on and so forth.

Eric Hess: [00:33:05] Yeah, certainly from a quantitative modeling perspective, you can certainly see how the Koopman operator, particularly with the time slices and the way that it collects data, having applications for stock and all types of asset quantitative trading. Now let's... let's talk a little bit about security. I think that's something that, you have been focusing a lot more of your attention to. So we get back to Mixmode, let's talk about how the Koopman operator facilitates what Mixmode is doing.

Igor Mezic: [00:33:32] The approach is the same as these, in these other applications. In some sense, I started this notion of useful information, and then that's the critical thing in the whole context of all these different applications, which is okay, we're measuring a lot of data on the network and the amounts are huge, but what is the really important part? And in the context of what we've seen recently, in the example of the recent breach that was announced and happened, you see that perhaps monitoring just or understanding just the aspect that the certain piece of software is calling out from the inside and it shouldn't be doing that is enough to understand that there is something malicious going on. But that perspective is a little bit different than what exists in network security in general today. In general, the network security software is based on the rules. So let's say you want to monitor for something like exfiltration. You say, if there are files going outbound, and if they are bigger than 30 Meg, which is a threshold, then sound an alert and if not keep quiet. That's a rule, right? An AI system would really say okay, let me monitor this network for awhile. Let me formulate, what is the normal behavior? Then let me find the deviations from that normal behavior and if the deviation is sufficiently big, I'll point out that there is a risk associated with this process. So we take that latter perspective, but an advantage that we have is by deploying Koopman operator theory, we have all these aspects of causality and learning over time and adaptive learning rather than giving the AI system just a bunch of labeled data and have it process it, and then that's the model. And if something new happens like you put in a new router, well you need to repeat the whole process again. So we've taken the approach to formulate the model of the underlying dynamics using the Koopman operator theory, then we can formulate the normal aspects of the behavior or the model understands the AI understands normal aspects of the behavior and then if something walks through that it hasn't seen it before, it actually does pop up a risk alert. And if it's seen as before, it's gonna show up in some notice that is surrounding contextually that event. But if it hasn't, that might be a zero day event where you are still detecting something, and obviously just like the kid not knowing that's not a cat, it's a tiger, there's still an alarm sounding off. It's just that there is not an immediate knowledge of

what that particular event is. And that can be labeled by a little bit of parenting later on and stored in the memory.

So utilizing the operator itself, we have this time variable. And so we can start learning from the first five minutes, understand what the system looks like. After a working week the AI has a very good idea of what looks normal on the network, but it keeps adaptively learning and watching for changes. And then, the labels themselves get put in as we go. You can obviously have a lot of labels and rules to start with, and we do. For the processes that are there it's templated data, but the core and the heart of the system is really this Koopman operator based model that enables adaptive changes to the model itself.

Eric Hess: [00:36:50] Right, so it sounds like maybe one of the differentiators versus a more traditional machine learning approach to the AI is that the Koopman operator allows for a dynamic network baseline to be established. And that dynamic component of it is better tuned to pick up deviations because it's constantly evolving.

Igor Mezic: [00:37:10] That's right. And the representation is simple in the context that it is linear. We pick up the aspects of the network analysis, coupling again, to what we talked about earlier. We pick up the aspects of the analysis, like for example, the weekly changes of daily 24 hour changes that are entirely linear. We pick them up on their own. We don't need to put in the frequencies at which things change and stuff. If there is a 24 seven type operation then that will actually not exist. But it picks them up on their own and presents this finite dimensional model and then once it has a model, it's easy for it to figure out what the deviation from the model is.

Eric Hess: [00:37:45] Excellent . Moving from security, another area that you've done a lot of work on is smart cities. Do you want to talk a little bit about your work on smart cities?

Igor Mezic: [00:37:55] Yeah so most of the work in the smart city context was in sort of smart buildings. And that is a very similar deployment as the one in network security. The difference is that the data in network security is digital, so it's packets. While the data in in the context of let's say building infrastructure is physical, mostly physical. Although of course there is a network as well that plays into the picture. So there is some aspect of cyber. And by the way, these two fields are coming together in an important way, because we do want security for the systems that run the building for IOT. So this was really... and this went early on from my engagement with the institute for energy efficiency here at the university of California, Santa Barbara, where we wanted to understand whether AI can help to run buildings in an energy efficient manner. And so we've deployed the systems... I think there was a point at which it's set up 42 million square feet, all around the world and on four continents. And that work is continuing as well. But it's a very similar idea in the sense that you have normal behavior that occurs when people come into the building and the energies usage starts going up and then they leave during lunch and the energy usage goes down a little bit. And then at six o'clock everybody leaves. And so the AI picks up those patterns, understands those patterns and then comments on the deviation.

Eric Hess: [00:39:18] Can we talk about how the Koopman operator in some of your work on the smart cities has evolved?

Igor Mezic: [00:39:24] Sounds good, so it was a similar application to the one that we have in network security because the data in the building for the systems, the internet of things systems that are running the building, they go along the backbone network like backnet is one of the types of languages that those networks speak. But most of the data that you get from a building like that is temperatures, pressures, ventilation, and the idea is similar in the sense that the Koopman operator approach can formulate the model as to what healthy operational building looks like. Let's say we have commissioning, somebody came in with building their engineers then fixed all the problems, and now it's operating in a very nice manner.

And now you formulate the model of that. And now the AI has a picture of it in its head. And if something starts deviating, let's say a boiler starts utilizing a lot of energy to produce exactly the same kinds of temperatures that gets reported and root cause analyzed a little bit on the AI layer.

And that helps the running of the system to be more energy efficient. So I think there are some really nice opportunities there to extend this to the broader range of smart cities , the water infrastructure and so on and so forth. We had the recent paper in nature communications that talked about utilizing Koopman operator methods to understand the traffic flow in LA of all places. We know that's the worst place in the world as far as the, traffic issues are concerned. We had some discussions after that with the California department of transportation on utilization of these techniques. So to my mind, those applications in infrastructure, smart cities are the ones that are hopefully going to bring the society an element of efficiency that we don't have today when the systems are designed, on a point basis, because the Koopman operator, one of the aspects is that it aggregates all this information and it produces the important components of that information. And what we think is an important component purely for traffic might actually be influenced by of course the work schedule, right? If everybody is coming to work at nine, your traffic is going to be clogged at 8:30. So those correlations of that type are pretty easily detected using these methodologies.

Eric Hess: [00:41:41] We actually did a show with Paul Clayson and he was the CEO of... he is the CEO of agile PQ for IOT devices, basically securing IOT devices. And as we talk about smart cities and the work with mixmode, obviously there's an explosion in the number of IOT devices. And there is an increasing alarm being sounded by various security professionals, that these are just largely unsecured there's vulnerabilities, and this is a growing concern in the marketplace, because all this information in the aggregate one, it could tell a lot of information about the people utilizing them, allow them to be hacked. We talked about an example of some of the vulnerabilities, allowing a third party actor into your whole network just through the IOT device. And then there's also even the potential of, as they're being deployed on buildings to monitor temperature or critical processes. And the disablement of them could cause a severe economic harm. So when we think about all that data and the impossibility of a human actually monitoring all that themselves. It's just, it's one thing to monitor a large corporate network enterprise system. It's another thing to take in disparate, tiny points of data from all over and try to correlate them into a

use pattern because their use case and the more there are and the way that they're used are truly chaotic. How do you see the Koopman operator facilitating a model that better secure IOT devices?

Igor Mezic: [00:43:09] Let me put this in perspective. The current model that we have for securing devices are untenable, exactly because of the aspects of what you pointed out. There is a lot of them out there and they are different. And the writing rules for all of them, different rules for an exponentially exploding number of ways hackers can come into devices, it's not a route that's going to yield fruit, because you're constantly lagging behind.

Eric Hess: [00:43:37] The growth of IOT is going to extend well beyond man's ability to adequately forecast or try to feed data into a machine learning algorithm.

Igor Mezic: [00:43:46] Exactly. So I think almost by pure pressure of the situation, the algorithms that we need to think about are the ones that adapt on their own, that are like humans in a very limited sense, right? That adapt, take the feedback from the field, adapt on their own and have procedures to alert either the user or prevent the further exploit on their own.

I really think that's the only way forward. I don't think that, the expert systems, the first wave AI rule based systems can handle this for much longer. Now the operator theoretic approach is one framework that has those properties, right? That the other AI frameworks currently don't, which is it can learn from very small amount of data.

And it can build its base of knowledge adaptively to the new data without the need for a huge relearning process. And I think that's going to be the key to provide security layer for those devices. Now, of course, people are smart and people who break into devices are smarter. They're always possibilities finding new ways. But the argument that I'm making is that we need behavioral imitation of our AI to the adaptation of these new methods that the hackers are using and they are going to be using a lot of AI as well.

So I don't really see how the deployment of methods like this, being Koopman operator theory or others can be avoided. It's almost a forced function, right? One has to do it. We have to develop those methodologies.

Eric Hess: [00:45:24] Right, and as there's more devices and as it gets more complex, it is truly chaos.

Igor Mezic: [00:45:31] Yeah. It's chaotic. You're collecting all of this data. Most of it is chaotic and Koopman's language would call it a continuous spectrum and it's... it's not meaningful to extract the data from, but what you can do is you can contrast what you have in this whole chaotic behavior in the model versus what you're seeing now.

And if there is a difference, something going on and AI can zero on, rabbit hole that and extract meaning from it, then that's precisely the architecture that we have in Mixmode.

Eric Hess: [00:46:03] It was pretty clear that the world's going to continue to need people like you to help us with all this. It was great to have you on the show. Thanks for being a

guest and teaching us about the Koopman operator, an operator I would have otherwise probably not known anything about, so thank you.

Igor Mezic: [00:46:17] My pleasure. Thanks for the conversation. It really Illuminated a lot of things that I probably thought, but didn't have a great way of bringing down so I hope that some of these aspects came through clearly and thanks for having me.

Eric Hess: [00:46:31] And if we want to, if the listeners want to learn more about you, about what you're doing about Mixmode , where can they get all that information?

Igor Mezic: [00:46:38] Oh, so mixmode.AI is a good website. My webpage at UCSB with my group on nonlinear dynamics and operator theoretic methods in nonlinear dynamics and control theory. Those are two major places where they can find out. And then of course research papers like on archive repository are a good place as well. Or just send me an email and I'll be happy to respond.

Eric Hess: [00:47:03] You want to give your email address?

Igor Mezic: [00:47:05] Sure. It's just my last name@ucsb.edu.

Eric Hess: [00:47:08] Excellent. Once again, thanks so much for coming on the show.

Igor Mezic: [00:47:11] Of course. Thanks, Eric.