Estonia: The Rise of a Digital Nation. Dan Bogdanov, Head of R&D at Cybernetica

[00:00:00] **Eric:** Since its independence in 1991, Estonia has transformed itself into a digital nation and a European tech center. But how that happened, we were fortunate to have Dan Bogdanov head of R and D at Cybernetica also a professor at the university of Tartu and inventor of Shareminds, privacy enhancing technology solution as our guest cyber net.

It's an Estonian company with a strong focus on research and development. It creates secure technologies for mission-critical systems and had an integral role in establishing the e-government ecosystem in Estonia. That includes digital identity, interoperability, internet voting. Now I've been meaning to get into Estonia on a podcast for some time and so much so that when I approached Dan, we decided to do two episodes.

One to focus on Estonia as an encrypted economy, and then in cybernetic his role in that, [00:01:00] and then shifting over to his work on Shareminds and privacy enhancing technology generally. And we'll be publishing that part of the episode in two weeks. So, I bring a bit of my. Into the main episode because I wanted to set the stage for that discussion.

So, we'll leave it here. Last note, a few acronyms PKI is simply public key infrastructure in RSA was one of the first public key infrastructure systems used. If you enjoy this podcast, please, as I always say, share, share, share. Thanks so much. And with that, I bring you a Dan Bogdanov

Hi, this is Eric Hess with The Encrypted Economy. Today, we have Dan Bogdanov who's the head of R and D at Cybernetica and the co-inventor of Sharemind, a database with built in non-disclosure agreements to secure. He leads a team of researchers and development [00:02:00] specializes in secure multi-party computation, priming, preserve privacy, preserving data analysis, and software architecture.

He is a Ph.D. in informatics and a master's in computer science from the University of Tartu. Welcome to the podcast in,

[00:02:18] **Dan:** thank you so much, Eric, for having me here and very excited about the discussion we are going to have.

[00:02:24] **Eric:** Yeah. So, I'm actually going to start the podcast a little differently. I'm going to drag a little bit of my intro just to sort of set the stage for my own fascination, with Estonia and Cybernetica and sort of what brought us to this place.

A number of years ago, working for a number of digital asset companies, trying to find appropriate jurisdictions happened upon Estonia. but Estonia was very different than some of the other jurisdictions I was looking at in that it required a little more engagement from an Estonian to form a co that kind of company from offshore, [00:03:00] which was, was a, a factor in limit.

But it also was in retrospect, an indicator of how Estonia views partnerships. And if you're going to come to our economy, we want to work with you. We welcome not just digital assets, but really all things encrypted. there's a strong focus on encryption and privacy in at the government level and at the private level and a real push to sort of drive that in the economy.

And, and I brought into the introduction because in many ways Estonia is the Encrypted Economy that my podcast is about.

I feel like they could be the model for other countries looking to do similar things and. It just makes me very excited to have this podcast. So welcome Dan, as a head of R and D at Cybernetica, and also somebody who's actively involved in the government there in a Cybernetica of being involved in the government, public private partnerships.

[00:03:56] **Eric:**

So, Dan, before we get [00:04:00] into the rest of the podcast why don't you give us a little bit about yourself

[00:04:04] **Dan:** Indeed. So, I started using computers at an early age. My father and father brought me a Commodore 64 around the formative age of 10. And I learned to do some basic programming pretty much after that.

And that became a lifelong hobby and interest, which made me write computer games for various platforms and build the sort of manual skills needed to build software. So as of logical follow-up, I went to the university to study computer science and did a bit of work on the site, worked on things like healthcare systems.

And that gave me a good understanding of the privacy and security aspects of any data-driven system. So, I decided to take my research towards cryptography [00:05:00] for my master's thesis. I have a first draft of the Sharemind secure multi-party computation system, which I then continued to work on for the Ph.D. And also, I've been

working on privacy technologies and security technologies ever since. So been a computer user since an early age and have some academic degrees.

[00:05:26] **Eric:** Excellent. Excellent.
So, and you know, I talked a little bit about, Estonia. Maybe we should start off really thinking talking about the history of Estonia and, and why did Estonia take the lead on cryptography and digitization?

Like what, what made it a prime country to do?

[00:05:51] **Dan:** So there were multiple aspects, and the people are still figuring those out. And the hypothesis and theories vary, depends on who you [00:06:00] talk to, but consider for a moment. after 1991, when Estonia regained independence from the Soviet Union, we were at a situation where we almost had no significant technological legacy when it came to IT. And that was a bit of a boon, really. That is a good thing because we could start building things from scratch based on the techniques that were already available. So, there were institutions like the Institute of Cybernetics at the Estonian Academy of sciences, which was a sort of a governmental let's say technology lab where various new technologies were prototyped proofs of concepts built research papers written and so on.

And you could see that Cybernetica as a company is a [00:07:00] spinoff of that academy of sciences lab because the people who wanted to build practical things in 19 97, 24 years ago, founded Cybernetica the company. In around that time we started reading cryptography books and started thinking of how the future of a digital nation should work.

What are the security fundamentals? So, our development leaders back then started thinking about how a digital government should operate. How should data exchanges be built? And while obviously, we had some foreign systems to look at, there was PKI, there were already things like RSA and all of that. That was, and that was a given we still started thinking about how that works for organizations.

So, in some of the early research papers published at that time, we see the foundations of the X road, the whole [00:08:00] idea of distribution, how you don't have to pull data together, how you can make a data services interoperate between government agencies, how you can connect the silos as some like the same.

so

that is the context. People started reading up on the state of the art and decided that we'll use the state-of-the-art to build the digital Estonia, the e-Estonia.

[00:08:30] **Eric:** And is there is sort of a unified view in government to push the E in Estonia? Ford is a very progressive government from a technological.

[00:08:39] **Dan:** Well, back then it was a, it was like bleeding edge, progressive. I would say these days, every time the government tries to seem to fall behind the bit, then there's sort of a societal uproar in the media saying that our, the Estonian it tiger is falling asleep again. And then yes, again, they have [00:09:00] to start building things and updating things, but there is now also significant competition.

There are many countries building some of the types of services that. Estonia hasn't built yet. So currently the focus of the government here is building proactive services, meaning services you will need, but you don't still know it yet, but at some point the government will come to you and say, right, you are in this sort of situation.

Maybe it's an age based trigger, but you might need that level of support. Here are the, here are the forums. You can fill them out, but the government comes to you and says, yes, you should do this. Estonia is not the first country to do this. There are now also others. So, the competition has really picked up and we're very happy.

It has because when there is a lot more to learn, there's lot more to share. There are full conferences where leaders of countries ministries working on it are coming to the talent, [00:10:00] digital summit, as it is called to exchange views. See which kind of open source projects are interesting. And how everybody else is funding all of this.

What's the latest on securing this cyber security aspects and all. So, yes, I would say that the government continues to be progressive and continues to invest. It's also because of a clear need, because so much of the system is digital that you have to keep it working.

[00:10:30] **Eric:** I know when we had Tom Attema from TNO on the podcast, he talked a bit about that very thing.

In terms of using privacy-preserving models to take into those and data in a way that was that, that the people would be comfortable with. but also using it as a tool to deliver need-based resources based on the analysis of data in a way that [00:11:00] would violate their

privacy rights.

So GDPR compliant and in
the like so that's that, that model was
really interesting, and Estonia has a couple of things that it's
really pressed hard within this country,
one being this notion of e-residency another one being e-voting could you do you want
to share a little bit about what
Estonia has done in that regard?

Certainly, just to
follow up on that privacy thing, then there is a project we are currently
getting to the conclusion towards, which is the use of artificial intelligence in
governance. And there were some of the core things that we have been working on
are how do you build models based on a population, and then use it to make the
work of a government agency.

More efficient or to
make the life of a citizen better. So, this is something we're [00:12:00] heavily working
towards
and there have been some well rather obvious findings, which is that technology
can't solve ethics. So sometimes you can't go to a person and say that, Hey,
our computer model says that you might be out of a job soon.

Maybe you should be
getting unemployment benefits. Here are the forums. and
the person might get the total shock out of this. So that is something that will be
a balancing point even with technology.
But coming back to the question around the internet voting and

internet voting is one
of the more, some would say controversial services available in Estonia and
indeed internet voting is heavily used
first to understand what does it mean? It means that people can vote for local
elections in local connections for their municipalities, for parliament, [00:13:00] they can
vote using a
computer wherever they are.

They don't need to go to
a polling station. They can be elsewhere. It's like mail-in votes, but doing it
synchronously over the internet. And that is technology-enabled by
pervasive use of digital identity. Government-approved government-supported digital
identity, which gives a really good level of assurance that a certain person is
indeed who they claim they are.

And internet voting. It has
reached up to 40% in recent elections, meaning that 40% of votes are
coming in over the internet from people's computers. And we've been doing it

for over 10 years. Now, obviously, the early versions of that technology were a lot more basic than that. Today's versions are with [00:14:00] significantly improve the protocols, given that the attacks have become more mature.

And you can now validate your votes on a separate mobile device because it's not reasonable to expect that your computer you're using to give a vote is a secure device to verify it on. So, the idea is to have a
a separate device, which hopefully isn't corrupted in any way because your a computer might have a virus, but then the phone won't hopefully because corrupting two devices of the same person at the same time, it's just so much harder.

So, this is how we've been working on
developing internet voting as a technology. We're up to hour. How many of the operations? Fifth, six, something like that. And the development goes on. E residency is another recent innovation, which allows citizens of [00:15:00] other nations to do
business that's in Estonia.

One could make the
analogy of sailing on the seas. If you have a ship, when
the question is under which countries flag are you sailing. So, the question with e-residencies, you might have a company under the Estonian flag, and you are operating that company under Estonian laws, Estonian business but you're not a natural Estonian citizen.

You're an e-resident IE
going for electronic digital. They are onboarding process for becoming a new resident is a pretty significant, you have to give an Estonia sufficient grounds of trusting who you are, and thus it is available to many countries in the world, but the process still takes a while. But once you've done that, then it becomes possible for [00:16:00] you to have a business in the European union and run it from abroad, using digital signatures, using mobile ID, the smart ID, the authentication channels available.
You can interact with a government fully digitally.
You can interact with the bank fully digitally as well. So that is something which has brought a lot of companies to Estonia. some
of them, not, all of them have been fully honest, and these have been found when they are trying to do something that's illegal.

Then obviously this is
not what the e-residency program was for. It is in no way designed to be a sort of a Haven for it, legitimate uses, but
it is instead a showcase of what is possible if you build your technology just right. And this circles back to what you said in the beginning that Estonia and might in some ways be a [00:17:00] model and Cybernetica.

It does a lot of work
internationally. We built systems, digital ID, government technologies in various countries in Asia, Europe, middle east Africa, south America. and we see that we can't be a model for
everyone because countries are actually different. The governance models are different.

The maturity levels are
different, meaning that in some places they can take certain parts of what Estonia users. But we do not think that cloning Estonia as a whole country is a reasonable course of action for most of the states on earth. So instead. Look at what they have, what they need. And then we try to put things together from pieces and might be that a certain things that work in Estonia to not work in other countries.

And we are very mindful of that. And [00:18:00] then we do not force them on anybody.

So, so we'll double click a little bit more on e-voting,
but before and e-residency, but before we leave, the residency has Cybernetica had been involved in the residency program with the government,

[00:18:16] **Dan:** to a
limited degree, certain amount of consulting reporting.

but we
are, it has been driven by other great people.

[00:18:26] **Eric:** So, in terms of the
residency, what would be the difference between, I guess, forming a CA a foreign entity forming a co a company in Estonia? I
don't know if the participation of an Estonian citizen is sole or reserved,
still required. what would be the difference between that and he resonant, right.

[00:18:48] **Dan:** So, let me give you a,
like a sort of an ideal scenario. The key about this, eh, that is not always obvious is that [00:19:00] a lot of things can be done over the internet digitally using Estonian e-government services, founding a new company. If you have your papers at hand is done under an hour, In Estonia, you can find a new company.

Somebody actually did it
in 18 minutes, so they did a speed run. But the point is that this is something that's available to you.
You're sitting in a cafe and you're founding a new company for the business idea. You just got with a friend 15 minutes ago, and this is what you can do.
If you have the access to that digital identity, your contract with the government, they know who you are.

You're founding a new
company. You may have access to certain level of banking already. And you can do that. This is not always clear because otherwise, obviously you can come to Estonia. You can show who you are. You can start [00:20:00] convincing the local boards that you want to find the company here, and you are going to be a foreign, a foreign national while doing so and all in all in all.

But the point here is
that you go, you do e-residency thing in one of the stones and embassies, for example, and then you're good to go. There are certain parts in the banking sector, which a certain extra
hurdles that you might have to jump through because the anti-money laundering controls are pretty strict,
and these still need to be enforced.

However, this is still the level of ease that we've implemented in running a business. From abroad is I do
believe unprecedented.

[00:20:47] **Eric:** Right? So, so to, to
draw the distinction as I understand it because
I had formed a number of companies overseas and typically particularly these days you know, [00:21:00] there's a due diligence
process for each company you seek to form
there are gatekeepers which are
the law firms or some entity formation.

and,
and once you've gone through the gatekeepers, it could be easier, but the gatekeepers are effectively almost like an agent. They'll say, I want you know, three forms of ID. I want your
passport. I want a recommendation from your banker. I want a
lawyer or an accountant to sign off on these things.

I want very detailed
information and it's a bit of a hurdle and if I want to then say,
okay, I want to form another company. I sort of have to do the same thing. I
kind of have to use the same I might be able to leverage some of the prior
materials, but I still have to go through
I still have to go through a gatekeeper
to do it.

what
it sounds like is that if with the
residency once I've sort of established.
Myself as a founder of, let's say a founder of a [00:22:00] company I've applied
for residency, and I've been granted. It it's easier for me to then you know, I basically
plugged in its, it's sort
of like I'm in the U S I want to form an entity in the U S that process is
always simpler than forming an entity overseas, but because there's, there's a
Morty plugged into the system, I can leverage everything.

I don't have to go
through the same process where the gatekeepers it's relatively easy for a U S
citizen. my understanding from what you described is
that relative ease would now exist as if you were an Estonian citizen, trying to
do the same thing.

[00:22:35] **Dan:** Yes. That is exactly it
sort of bootstraps you into the same digital economy, but we are running here,
and you don't get immediately the same rights.

There are certain
constitutional things. We do not try to be residents. And then there's the next
question of whether you get health care, whether you get to put your kids to
school and so on and so on, but that's sort of a future work for that [00:23:00] program.
The initial
design is indeed to run businesses, to run businesses within the European
union, which is a pretty good place to run certain businesses.

And ease of access is probably, let's say the
overhead of running a new business from Estonia using E residency is probably
one of the lowest. And the issue of gatekeepers is especially strong here because
efficiently there are
rules. If you, you, you're given a computer form, you're given an online

service, a website, which tells you what you need to show, what you need to do.

It's sort of a digital Cate
gatekeeper. You could say, however, it's highly automated and the people in the backend while they do check for your sort of the identity checks and the checks of your trust have also been done when you applied for the e-residency. [00:24:00] So once you, once we've
established that, then we assume you're good.

We put certain trust in
your ability to protect the tokens. We identity tokens, where Estonia gives
you. And given that you do that, then afterwards, we sort of we accept you as we accept you as one of ours. Let's say, just
say very bluntly, I guess. And there's
um there's a sort of. The financial
side, how much you had to pay for all of that.

That's also sort of not at the whim of an agent of some sorts.
Obviously they're already consultancy companies, which make the whole, let's found an AI, found the company while you are a new resident thing easier. They also handle the accounting and reporting for you. So, there are there is already an economy around providing
support [00:25:00] services for e-residents, running companies.

And that all also is
unlike an extra additional layer of ease on top of that because they also handle your accounting for you and everything. So, it's sort of a, you can find a one-stop shop these days, but does something like that.

[00:25:18] **Eric:** Excellent. and
then now switching back to voting now, I
think from what I recall, Cybernetica, I was more involved in the construction of the correct.

[00:25:29] **Dan:** So, we came up, we've
been, we've been building the Estonian e-voting system since, since its Genesis pretty much the first protocols were
rather easy. They were, well, it can, if you can imagine like a mail-in vote, you have first, you, you vote for someone, you put the name down on a piece of paper, you put it in an envelope, you do not sign the envelope and you put the

envelope in another envelope, you sign the external envelope.

So that's the sort of an
idea if you would like too then. Tally [00:26:00] the votes. When you
look at the, you collect the envelopes, you look at the envelopes check. If
it's a valid voter, if it is you take out the internal envelope and put it in
the polling box, and then you can open the box and counter votes, but you won't
have the names on them anymore.

So that's exactly what
was implemented in the first version of internet voting, using standard
cryptography, public key asymmetric cryptography, the internal envelope is encryption.
You encrypt the vote
and then you digitally sign the encrypted vote during tallying you just check
for signatures and you're you throw away the signatures.

And in the box, you just put the encrypted votes. And
then at some point you open the box and decrypt the votes and check. So that
was the first, that was the first protocol implemented. You could, you could
explain it to your grandmother back then [00:27:00] these days, it's all
about mix nets, bulletin boards, zero-knowledge proofs, and all of that because
you need, you have a lot more threats
you want to defeat.

You want to trust a lot
less people trust against the government has been something that Estonia really
has had when we regained independence,
when trust against the government was rather high and. But then you could,
government could get away with a lot of things. in
point a positive way. I would say these days as maturity increases, people understand
things better.

They distrust against
certain government agencies can also grow and thus building protocols that, um allow
you to trust the government less is a
worthy design goal. So that's where we're aiming for now building protocols
that allow you to trust your [00:28:00] government less. And that's a sort of a driving point
under some of our privacy work as well.

That even if the government
says that they will build a COVID-19 contact tracing system, then it would be

really nice if they build one that they cannot repurpose as a surveillance platform later, once the epidemic has passed, for example, things like that. So, there's a whole thinking about how big infrastructure pieces do want to build using computers and the internet voting is a significant piece because arguably it can significantly change outcome.

obviously there's a lot of discussion on, I don't know, can your neighboring countries, for example, certain large ones to the east of Estonia mettle with your votes and change the outcomes and get friendly parties to power. And these risk analysis have been done both from an economic standpoint and then [00:29:00] from a non-rational standpoint as well.

And there, isn't a clear understanding that this is something that we're doing now. There's also a social aspect here. If you want to get people to the polling stations, young ones, folks who are used to the new style of living, where things are digital against get everything from the internet. And so on, then a voting is just another thing that works for them, and it allows them to do the voting also when they're working abroad or traveling or anything.

So that is something which is a sort of yeah, that's the thing. It's like the, a common example of declaring taxes. we can declare our taxes online. It usually comes pre-filled. And for people who are not doing any investing or don't have any foreign incomes when usually the tax declaration is five minutes that's because they all the employment taxes, [00:30:00] all of aunties already there, and the Estonian and tax and customs port has already prefilled that form for you.

And you can do it on your mobile phone while you're resting in the Caribbean. So that's the idea you are in Estonian wherever you physically are. or you can be an E-resident wherever you physically are, but you're running an Estonian business. It's sort of a same, same international global view on how you run things and how you provide yourself.

What, how do you
interact your citizenship or your residents in that regard?

So, we're going to,
we're going to come back to the toolkit for e-voting later, but just to
highlight, you mentioned zero knowledge proofs. What other privacy enhancing
technologies are
incorporated into the voting system?

there's some there's [00:31:00] mix nets, mix nets are
very helpful.

If you want to hide the
sources of certain it's like shuffling,
it's like shuffling a ballot box. Think of it like that. And there's obviously
various encryption and probably there are some things more than I don't
remember off the top of my head because that protocol was again changed a few
years ago.

And I just have to
admit, I don't know it, but you can find the source code on GitHub. That's the
nice thing. You can go and find it and you can technically roll your own voting
up if you really want to. And it should be compatible with the backend. And if
it is when you can compile your own voting app and run it and
you'll get to vote on something, you compile it yourself, which is pretty new.

Most people still go for
the government delivered version for
ease because not everybody in Estonia is very good at building software off of
GitHub. We're still working on that, but that was a joke. But, um but the point is that
[00:32:00] technology is, there are more and more coming
here. And for example, let's just
mention blockchain.

Let's give a nod to
blockchain. Timestamping was Cybernetica
built its first timestamping linked
timestamping service in 1998 or
something that's what's called permission blockchain today, I think, or it's
very close to that, but timestamping is sort of like a service, which tells you that this, this
document existed at that date and

time.

And we have a timestamp
on every digital signature given in Estonia because obviously you shouldn't be able to backdate your signatures. You can do a lot of fraud this way and new technologies. We start looking at them,
prototyping them building proof of [00:33:00] concepts at a pretty early technical readiness level.

So, our Cybernetica provided public linked time stamping service, like a notary service was the second in the world. The first I believe was built by Surety in the United States and we built the second one. it
didn't get much traction back then because obviously we're a little bit early to the market.

And well, these days there are companies who earn
a lot of money by doing something like this. And people are building whole businesses across on top of that. The point of that was that technologies have their place in time and the privacy technologies are now finding their time Cybernetica. And I, me personally, I've been doing privacy technology research for the last 15 years.

Initially when we
started going around with thoughts like
secure [00:34:00] computers, A multi-party computation, things like that. Then folks looked at us and said, this is really awesome research. It will be needed very much in the future, but we couldn't get serious proofs of concepts done. Then around 2011, we got our first real applications, 2016.

We got our first like
governmental applications done using MPC and now the technology is mature enough that we are putting it on more and more roadmaps for inclusion in the future. And well technology has come up
all the time. There's data synthesis and there's trusted execution environments and things like that.

And well further they will be, they will be implemented based
on a business need, I would say. And that here we find an interesting innovation [00:35:00] innovation question of
if you have an existing system, but you know how to build a more secure one, then what is the lever? What is the, what is the sort of trigger that should inspire you to

rebuild
your existing system into a more privacy preserve?

for
example, right now, if Estonia started from scratch right now, I think we would have a lot more privacy technologies in the government. So, we've already to some degree sort of not, I wouldn't say fallen behind, but we're not starting from scratch these days anymore. Now we, if we take something, we already have the business logic in place.

We have the service in
place, but we would need to sort of iterate. And when maybe when the next big implementation is done, maybe it is built on secure computing. This time could be. So, the government has been using secure computing for certain analytical studies. And [00:36:00] there are plans for using it to analyze certain rolling delicate data like mobile phone
location, data for statistical purposes.

And well obviously the COVID-19 contact tracing
app was based on privacy technologies. the Estonian version was using the apple and apple and Google implementation which
used Bluetooth fans, a lot of clever cryptography to ensure that basically the backend didn't really have much data at all.

So, I would say that
this is an ongoing process.

[00:36:37] **Eric:** So public private
partnership that you had with Estonia , Cybernetica I had with Estonia, how did it extend beyond e-voting?

[00:36:50] **Dan:**

I wouldn't say that
there's an exclusive partnership that Cybernetica enjoys. We do have a certain reputation and a certain expertise, which is rather [00:37:00] unique, but mostly about cryptography. So, we've gotten to build a lot of systems, the Estonian e-government the interoperability system between an Estonia unique government services.

The X road is initially
a Cybernetica, a design these days. We are not maintaining its code base
anymore. That's now managed, handled by the government and actually there's a
whole Nordic interoperability. which
runs with, and ensures that it goes in
the right direction. but we were the ones who built the first six
versions, I would say, so that, and also maintained and run it.

then
there's the identity platforms. We've built a cryptographic underpinning of
smart ID, which is a threshold RSA based mobile phone authentication and
digital [00:38:00] signature solution, which is rolled out to 3 million
people in the Baltics used. I use it to sign employment contracts every, almost
every day, but every week I signed a few and that's been something that we have
worked on various other identity
projects, like the original digital, um the ID card project, the PKI based ID card
that Estonia has.

We were related to the pilot of that. And well, we've
also been working quite a lot on the systems, the tax, and custom systems, for
example, and a big governmental access control and identity system. So, it's
not only the crypto work. We build all kinds of mission, critical software. And
it's been we have been a good partner for the Estonian government,
and They continue to work with us, and
we've been able to [00:39:00] transfer this trust to other governments internationally.

We have very good collaborations lengthy ones been going on in Ukraine, also
like building the e-government for African nations of Namibia and Benin and so
on. There's more and more there. So, some of the pieces of the Estonian model
are easier to export and others less. So, for example, Estonia has something
which is called the population registry, which some countries consider, or I
would just say heretical it's sort of a
list of every person with an ID.

And that same idea is
printed on the ID cards that we have. And if I'm interacting with the government, then
I'm technically proving to them. But I am the person with this ID because you
know, names can, names are not a very good, unique identifier. Many [00:40:00] people
can have the
same names, but the ID codes are designed to be unique.

And you get one when
you're born. It's actually to the level that I have two kids when they were born, they were assigned. The national ID codes at the hospital. Then I went home. They didn't have names yet. And then I could use a helpful online service to give them names. It works like this, but we figure out what the proper name would be.

And then we tell them, yes, that's my, this is my kid.
These are I'm trying to name the kid
with this ID code it's or, or helpfully.
They already tell me who my kids are. The forum actually shows me yesterday. These are your kids. You can name this one. And then me and my wife, we had to digitally sign it.

So that's, that's the
level of things we do. I named both of my kids online and got the birth [00:41:00] certificates later by
mail. And I sort of picked them up at the municipal government, but it sort of gives you the understanding that
not everything we do is immediately transferrable because a certain, the concept of a population registry wouldn't fly in many, most of your object, most European countries, you can argue that a lot of them actually have something which looks like a population registry.

Maybe it's a tax cut tax
number or a social number, like healthcare, like insurance numbers and things like that, which are actually pretty much the same. But you can argue that not everybody has them. then you obviously have to start the
discussion of whether everybody needs healthcare and whether everybody needs socially insurance or some taxes to pay taxes.

Usually, people need to
pay taxes. So, they need to have some sort of a tax number. but
they public arguments around this still
that ID numbers for people, [00:42:00] are
supposed to be pseudonyms. But in
Estonia they're unique identifying vectors, let's say. And they are not private in us. Social security
numbers are confidential as far as I'm
aware, for example, and, and in Estonia, that is not the case.

You can't successfully
impersonate anyone by knowing their ID code. That's where the whole, the

cryptographic proof mechanisms come in. You actually need to prove that you are the person with this ID code, just knowing the code or being able to show a document might not be enough to give you a digital access to services.

So again, we've built all of this deep from the ground up. We built a holistic approach to this, and it wouldn't transfer everywhere. if you build a holistic system and you make it a part of your society, then you are then you need to keep maintaining [00:43:00] it. And you can't really go back to driving horseback. Once you've driven a car, if something happens when you've fixed the car, you don't go back on horseback.

So, a few years ago when it turned out that the manufacturer of our ID cards, which are the thing you use for elections or signing documents or naming your kids online, apparently they had a floor mint, which meant that their RSA keys were incorrectly generated. There could have been. And the researchers from the Czech Republic alerted us to that mathematicians.

They had found this, and we had an election coming in like six or seven weeks, which meant that the first question is to cancel. Do you delay the election? Do you stop internet voting? What do you do panic? So, what Cybernetica good did back then was we helped the government and other private companies well-versed in these technologies to [00:44:00] quickly build a, to quickly bootstrap on top of the initial ID card hardware and new kinds of keys.

We sweep, we swap the RSA keys out and put the elliptic curve keys in the hardware allowed for that. And then we went on, we fixed the car. There was a big issue. There were court cases with the chip providers because it was their fault, their fault, very old obviously, but the thing was indeed that we went and we understood that this, there is no way back from where we are with this.

There is just forward. There's just improving the security. There is adding new privacy features, whereas increasing trust, various reducing single points of failure. There's there, that's where we are. That's hopefully

that's what you have in mind. When you talk about encrypted economy.

[00:44:51] **Eric:** Yes. and,
and what about the government and
homomorphic encryption now, before I even put you on the spot with that, I'll [00:45:00]
say the U S could certainly
do a lot more from a governmental level
with homomorphic encryption, particularly it has, it's a reg regulates across
multiple financial markets and equities, commodities futures, all that good
stuff.

and it
has a singular reporting system known as
CATS, where everything has to report to a singular database, which by the way,
every single exchange also draws from, for its reporting. So, you have a lot of
different touch points, compelling case for homomorphic encryption, because
obviously that's a huge honeypot.

So, my, my question is does the Estonian government look at
homomorphic encryption as a potential solution for preserving privacy within
the government? Or, or is that still, maybe down the road?

[00:45:46] **Dan:** It is down the road.
And what we've been building instead on is a secure multi-party computation,
which is like homomorphic encryption, but within a distributed manner, morphic
encryption gives you the [00:46:00] ability to calculate on cipher texts, right?

Multi-party computation
gives you the same thing, but it also gives you a consensus system on what is
being computed. And that's an extra sometimes if you want to enforce policies,
like only calculate these algorithms or these functions, then. A multi-party computation
might be a slightly more compelling offer.

Also, it used to be that
multi-party computation outperformed, homomorphic encryption by several orders
of magnitude for more complex algorithms. This is a changing just today. I read
of a new, very cool pre-print on a
homomorphic system, hardware accelerator, which is making homomorphic system or
morphic encryption, a number of orders of magnitude faster.

And that was a very
exciting greed. And that might actually change things quite a bit. It will
require custom hardware. So, there will be it will take time until the cloud providers
and everybody deploys this, and it actually becomes [00:47:00] available as a commercial
offering, but still very
exciting development.

So, it's public. Yes, it
is. It is. It was, it came up just like, just read it this morning. On nights.
F1 was the beginning. It came out from LA a lot of the respected folks at MIT
and elsewhere. So, by believe it comes
from the DARPA homomorphic encryption hardware acceleration program. That is,
but that's really fresh.

So, we keep up, we keep
ourselves up to date. There's an internal list where people post the cool new
things in cryptography and, and the company tries to know what's cool. So, we have
 we built the prototype of a value added
tax fraud detection system. This is not totally unlike sales tax, but it gets taxed at different
points in time.

And he actually broke the system with a [00:48:00] tax office in Estonia on her trying to
make it so that the
government would collect certain tax declarations in an encrypted matter
manner, and then find fraud cross-reference and find fraud from them without
having to, without decrypting them, without learning all the transactions, but
finding people who could be avoiding tax.

So, this was actually
Cybernetica, did not pilot with the government using our Sharemind secure
computing system. That's the trademark we have for our sort of a homomorphic
secret sharing multi-party computation system. But that is certainly on the body, certainly
on
the roadmaps because we've found that given the very deep integration of technology
into our
society, then.

 we are
sometimes being considered as not having any privacy at all, [00:49:00] which isn't fully
correct there. We don't have super centralized, super databases in Estonia. In
fact, all the different government agencies still hold their own silos and the
X Road platform, but a Cybernetica design back in the day was exactly designed

to build transactional services on top of distributed databases.

That was its whole
point. And it's still being used to this day. But we, what we found is that the
data science and AI applications, which are again, becoming a lot more active
today is Estonia does have the governmental AI program. they
are much, again, trying to figure out how to pull all this data together
because that's how, that's how data scientists are taught at universities.

Today. You need to have
the data in front of you in one location and then you know what to do with it. so given
that we have a distributed data
architecture in the government and obviously we would like [00:50:00] to continue having
that
because it has served us very well. So, I see that the government in time we'll
need a distributed data analysis mechanism, or at least a secure computing
system based on MPC or homomorphic, encryption, or trusted execution that will
allow you to put data together without putting it to.

Or if it is put
together, then it's encrypted and there's policy enforcement ensuring that you
can't do anything you like with it. Once you've done it, it does take away
power from the data science teams. But that is a sort of a, that is an
interesting discussion, whether which direction the world is going, whether
we're going in a direction like countries like China are taking, when there's
our social scores to people, it's not,
it's like credit score, but for everything you do, whether you behave well on
the street or whatever.

And that's obviously a
big centralized system where everybody is [00:51:00] being graded on
everything they do, or there is this architecture distribution. And it might be that in one,
some countries and in
some governmental styles, one style wins out over the others. So that is an
interesting discussion. We will be having across the next few decades on
whether all the work that has been done in cryptography on a distributed
computing consensus, the programmable economy, all the blockchain networks,
tokens, all of that whether they will,
where it will take us.

Uh there's whether the energy overheads of some
blockchain style networks will actually force them to be. Let's say use less in

favor of more centralized blockchain networks. I would, I wouldn't like that because again, if it turns out that there's a single source of truth on the blockchain and it's [00:52:00] controlled by a single organization, then we're not very far off from having a centralized database, when you start looking at the trust relations of everything.

So, a lot of this is actually very exciting and we hope to play our part in showing that distributed still is the way

[00:52:18] **Eric:** and talking about the China and China's model. they also are pursuing a central bank digital currency which will also give them much more visibility managing data. it also appears that the U S now wants to move in that direction presumably not with the same designs as China's, but still with the desire to posit, to I guess ensure a dollar dominance and um that's probably one of the driving forces but also to facilitate programmability.

do, do you see that kind of initiative taking root in Estonia?

[00:52:59] **Dan:** The Estonian [00:53:00] central bank already has a digital currency, R and D program. So, we're not much behind on that. And I've been in some of these meetings and one of the things that I've always discussed there, and they've forced various the question of.

Controlling the cash issuing and also removal on the market and whether you want to have that controlled by a single organization, today's cryptographic technologies allow us to build them distributed networks of control as well. Meaning that either by, I don't know, going as basic as secret sharing or using threshold encryption for keys, you could ensure that no single organization can create new money or remove money from the market because that would be a pretty big problem.

Right? So, the question is exactly when we're talking about controlling money, then [00:54:00] are we talking about a single source controls or multi source controls? And that's again, following up

from my discussion beforehand, with who we build distributed systems or centralized systems and governments, which are going to be more centralized, might actually opt for more centralized controls over their central bank, digital currency.

Whereas others might
actually build actual networks where maybe, I don't know, in a pretty, as future vision, maybe if there's going to be a European union, central bank, digital currency, maybe all the nation state like member, state central bank heads will need to go and turn a key somewhere for actually any cash generation would be possible.

So that's sort of where
I'm hoping that maybe we can go because I believe that these are, and that's a great point that has been made by some
gentlemen from, I believe lunar [00:55:00] ventures is that privacy enhancing technologies should
actually be viewed as partnership enhancing technologies because not everybody is interested in buying privacy.

Well, some, if you talk
to some businesses and what's this privacy thing, it's this thing that Europeans thought out so they could do protect protectionist economy, right? So, it depends on your worldview in that
regard. But if you want to build proper partnerships, if you would like wall street, hedge funds, to be able to agree
on things on data, everybody puts some data in.

Everybody gets some sort
of market clearing price out, have auctions without having to put their secrets in. Then this is a technology that creates partnerships. It's not just privacy. It's a bit more, that's why multi-party computation is. in my
view, interesting, compared to homomorphic encryption, because of that multi-party control aspect, it achieves the same [00:56:00] encrypted computing, but it also gives you a need for some sort of a consensus model.

Outro

[00:56:06] **Eric:** So, this concluded the
first part of my discussion with Dan Bogdanov to hear the rest, please check in in a couple of weeks. And that episode will be provocatively. Privacy tech data and nuclear waste queuing off the notion that in many cases, while data

analysis, then the output of that analysis is what the enterprise or business wants.

What they really want to
do is avoid the data itself because of all the regulatory concerns and the privacy concerns associated with it. So, in that episode, we talk about the different types of data enhancing technologies, how they are adapting and how they can greatly enhance business partners. We also talk about cybernetic, a share mind, the secure computing and data and analysis platform.

We cover a lot of ground
on that episode and I'm sure anybody who's going to listen will learn a great deal from it.[00:57:00]