TRANSCRIPT

Global Partnerships to Combat Cybercrime & the Challenge of Going Dark

“Keynote Address”

RECORDING DATE
Thursday, December 5, 2019

SPEAKER
Ferdinand Grapperhaus
*Dutch Minister of Justice and Security*

MODERATOR
Catherine Lotrionte
*Senior Associate, CSIS Technology Policy Program*

*Transcript by superiortranscriptions.com*
Catherine Lotrionte: (In progress) – the minister had worked for a number of law firms, most recently before he took his government position the law firm of Allen & Overy in Amsterdam. In his work as a litigation attorney, the minister focused chiefly on collective labor disputes, works council issues, and individual employment issues. He also advised management and supervisory boards on governance. From 2015 to September of 2017, he was actively involved in the Allen & Overy CSR policy as chairman of its board. From 2005 onwards, he was also a part-time professor at the European employment law at the – and I am going to mess up the name of the university; I apologize – Maastricht. I know I messed that up, sir. I apologize. My students will be horrified. On October 26th, 2017, Minister Grapperhaus was appointed as the minister of justice and security by the government.

I would like us all to welcome the minister to the stage. And let’s hear – and I will reserve the right to ask the first question of you, Minister. Thank you for joining us.

Ferdinand Grapperhaus: Ladies and gentlemen, less than a mile from here, in the Library of Congress, you can find a unique treasure: the first map of the world to use the name “America.” It was made by the German cartographer Martin Waldseemüller and first published in 1507. And to be honest, the name “America” is placed on what is now known as Latin America. Anyhow, it was proof that the Roman poet Virgil was right, that there was a land that lies beyond the stars, beyond the paths of the year and the sun, where Atlas, the heaven-bearer, turns on his shoulder the axis of the world set with blazing stars.

Now, Waldseemüller based his map on the travels and discoveries of Ptolemy, Amerigo Vespucci, and – no surprise – Christopher Columbus, explorers who sailed the seven seas in order to discover new trade routes, new products, new trade partners. Indeed, also in those days money made the world become round. These men – yes, I’m sorry, all men – these explorers and cartographers made the unknown into the known, because in the unknown there were dragons.

Now, the world of these explorers was a world of land, sea, and air – dangerous but visible, definable, finite. In the last 70 years, we expanded that known world in two directions: up and everywhere. We went up in space in the ‘60s. In the words of President John Fitzgerald Kennedy, “We choose to go to the Moon in this decade and do the other things, not because they are easy but because they are hard.” And then we went beyond what is there into a new – into this manmade everywhere, which is cyberspace – invisible, indefinable, infinite, and just as dangerous or even more so than the old world, because cyberspace is not a place on a map. Cyberspace, digitalization is everywhere.

Over the course of just a few decades, the world has entered a digital age in which people from all over the world are connected online. In ‘96, only 36 million people used the internet, less than 1 percent of the world population. In 2017, that figure had risen to 3.7 billion, nearly half the world’s population. Individuals and businesses, governments, NGOs,
financial institutions, think tanks, we are all connected, and we all use these endless resources, the endless possibilities of cyberspace.

And I think that is a good thing, because digitalization brought us a lot – e-learning, e-health, unlimited information, shared knowledge, social media, Internet of Things – possibilities that seem to be endless – talking refrigerators, self-driving cars, and robots that can dream. But digitalization also brought us ransomware and fake news, the Dark Web, cyberstalking, digital espionage, and cyberattacks, and maybe even some Manchurian candidates we don’t know about, killers instructed through the internet somewhere out there. Yes, cyberspace brought us cybercrime and the need for cybersecurity.

And to be honest, our society meanwhile has become almost totally dependent on digital resources. Critical processes like telecoms, water supplies, financial transactions are now completely reliant on our digital systems and processes. If one link in that chain breaks, it soon may have a domino effect. It will have direct consequences on critical processes in business and government, the earning power of companies and the daily lives of our citizens, not to mention indirect consequences. And the chain can break, and there are threats that will happen on purpose.

Such purpose comes mainly from two categories of perpetrators: state actors and criminals. Their influence and deviousness is growing and continues to develop. State actors who try to digitally influence elections, but also reputations and public views. State actors who may even want to influence essential processes in society or even sabotage vital infrastructure, thereby undermining free society.

Criminals present other threats. Let us first take a close look at those. They continue to develop criminal revenue models such as ransomware, like in 2017 when organizations across the globe fell victim to a ransomware attack. In the Netherlands, one of the largest container terminals in the Port of Rotterdam were attacked, among others. Processes were halted and the delays were lasting for days, with severe societal and economical damages. In the United Kingdom, a more or less likewise situation occurred with two large hospitals.

And criminal organizations who have no technical – technological expertise can orchestrate a ransom attack. They just hire the experts to develop and distribute ransomware – easy money, but big social and economic consequences. And they also find people who can develop and distribute ransomware on the Dark Web. Dark Net, where one can find market that in the real world would be completely illegal. Markets for weapons, drugs, assassins, and, for me personally one of the worst, child exploitation.

And this is why our governments must put money and means into the investigation and persecution of those internet criminal organizations, as we did, for instance, in the cooperation between the Dutch, U.S., and German law enforcement to get a hold of Hansa. Hansa was one of the largest Dark Web markets in Europe. There were more than 24,000 drug products on offer, from cocaine, to specific sorts of MDMA, to heroin, as well
as a smaller trade in fraud tools and counterfeit documents. So, the Dutch investigator started an undercover operation with fake accounts. The Dutch police was able to take full control of the site itself. And from that moment on, they could keep a digital eye on Hansa’s buyers and sellers, learn everything about them so they could be identified, and even tricked dozens of sellers in revealing their locations.

It was a game-changing police intervention that packed a real punch against the Dark Web. Millions of dollars’ worth of confiscated bitcoins, more than a dozen arrests and counting of top drug dealers, and a vast database of user information. And that was an intervention that was only possible because of the cooperation with the U.S. law enforcement and the German law enforcement. And that type of intervention must continue, as must close cooperation, because to stand up against the increasing threats we must work with others – with other governments, other agencies, other countries, at political, policymaking, technical, but also operational level.

Cyberspace knows no borders. So does cybercrime. So we have to think global to continue to pack those punches. For instance, to do that against international networks that distribute child abuse images. That is an important issue for me, in the Netherlands, because a huge amount of online child sexual abuse is stored on servers in or attributed to locations in the Netherlands. Because we are digital hub, we have a high-end infrastructure that criminals misuse. And it’s my aim to break that spiral. Victims deserve no less. So I started to organize a roundtable last year with the large digital companies, NGOs, and scientists. And coming from that initiative, the sector itself decided to develop a self-regulating policy with a notice and take-down procedure. They will themselves see to it that unlawful content regarding child abuse is removed within 24 hours.

Secondly, we built a hash check service that allows companies, especially smaller companies, to clean their servers up. And thirdly, the Tech University of Delft made a monitoring instrument that provides insight into which company hosts how many child abuse images. And last but not least, I initiated a legislative process to directly impose penalties on companies that do not remove the content within 24 hours after a report of child pornography or child abuse, including everything that goes with it. And certainly, it’s not only the penalties, it’s only – it’s the naming and shaming that also will go with it for these companies.

And to make sure that it actually happens, it will be supervised by a new independent national authority that will have sufficient enforcement resources at its disposal. Companies who are directors who do not defer to this authority will be prosecuted. And all actions that will—must help to slay the dragon of online child sexual abuse. Slaying these dragons to be cybersecurity is an integral part of protection against threats in the digital domain, essential for safeguarding national security as well.

However, challenges to effectively combat cybercrime remain, especially the challenge of going dark. In other words, how do we maintain access to information and credible tools that our law enforcement needs to find these criminals? In Europe and the U.S., we have the same discussion on the use
of end-to-end encryption by platforms such as Facebook, Instagram, WhatsApp, and others. And everyone agrees that victims of online child abuse should have our societal protection. Everyone agrees that we should do everything to find the heinous criminals that are behind those actions and prosecute them. Everyone also agrees that we have a right to privacy and data protection. And everyone agrees that we need to be cybersecure.

So here you see that end-to-end encryption is both a blessing in protecting the right citizens, but it's also a curse in trying to prosecute the criminals. Many of the tech platforms have moved to use end-to-end encryption or are about to. And I do agree with people that end-to-end encryption is an important feature on privacy protection. But I also see how our law enforcement agencies are struggling with how criminals benefit from the shield of privacy.

And we need to find a balanced approach to protect the victims and respect one's privacy. And I wish to stress, only for that purpose—to protect victims of such heinous crimes as child abuse and child pornography. And we need to do this together with the industry and civil liberty organizations. And I propose to continue the dialogue with the tech platforms. And agree with your attorney general Mr. Barr that we need to call upon them to take the responsibility to keep the internet a safe place.

Now, until now I've addressed primarily cybercrime and cybercriminals. But of course, the issue is much broader. We also have to talk about cybersecurity, state actors, because everything is connected. And that is why two small cities in the Netherlands are on the United States list. And I'm afraid it's not on the Lonely Planet's list of places you must visit. On the country I must admit, they're quite boring little towns. I hope nobody from those towns is listening. But they are crucial security targets because in these two small cities undersea telecommunications cables land on the shore. Fiber optic cables that are used for telephones, internet, television, that connect Europe with America through the Amsternet Internet Exchange.

An attack on those cables can have serious consequences for international internet and telephone traffic. In November 2003, for example, a relatively modest defect of one of the cables caused major internet disruptions in the United Kingdom. A coordinated attack on multiple cables might paralyze half the world. And as we see, state actors of various geographical and political background have been willing to try to influence our cyber-dependent systems to destabilize or, as I have pointed out before, to even sabotage our society. It makes us realize how vulnerable we are. How vulnerable we all are.

For this reason, earlier this year I presented to the Netherlands a national cybersecurity agenda. A free society needs a basic level of cybersecurity to increase our resilience against cybercrime and cyberattacks. And we have to ensure that our capabilities and resources to address threats are working, as the question is no longer – as one of our most reputed academic institutions earlier this year reported – the question is no longer if a
disruption will take place, but when. And we have to be prepared for that always.

We have to make sure that cybersecurity is a basic consideration in the further development of our digital processes. Against those criminals but also, I stress, that against state actors. We have to make sure that citizens, businesses, and public authorities improve their digital security and that the government fulfills its protective duty and the digital domain. And I can assure you, ladies and gentlemen, to get this awareness across to the public is – you won’t believe it – but it’s one of my more difficult tasks as a minister. So at least we must work together. We need public and private cooperation, and national as well as international. I thought there was some cyberattack already beginning. You never know. Maybe from the people living in one of those towns. They will find you. OK. Or because this lecture also nice to have on the internet, I hear it is streamed directly. I hope not through the cables that are arriving at the Dutch shore.

We cannot just rely on existing laws and regulations on security. Cyber has its own dimensions. One could even say that cyber in itself adds a new dimension in our universe, and that does not mean that we need a whole new set of rules and regulations – absolutely not. But as a society we must reconcile the specific aspects of cyber with existing rights and regulations we have in our society. In that respect, I stress that new does not automatically mean different. Cyberspace is not ultimately the exception. It does not have a special status for exemption, or whatever. So we do not need to reinvent everything. We must simply export what we need extra and take upon us the challenge to become the cartographers of cyberspace. And we, that is society involving everyone who has an internet interest or who has a cyber involvement.

And it’s clear that although we cannot be 100 percent responsible, governments must take the lead in this. But again, in dialogue with industries, with civil liberties organizations, with everyone to see where we can get to together. And we have to commit to a secure and stable country by recognizing threats to critical interests, and increase the resilience of those interests, be prepared for attacks and crimes, crises, and incidents that threaten society, but also take the lead in gathering and sharing information and knowledge. For instance, by stimulating fundamental and applied research into cybersecurity, that not only strengthen our own security but also to enhance our national and international knowledge position and our digital autonomy.

And I said before, government must take the lead in public-private cooperation. And that has already in the Netherlands, I can assure you, led to many great public-private initiatives and results. I named you, for instance, earlier on this code that the internet companies already agreed on after we had a roundtable on voluntary measures in taking of child abuse materials off their servers. So we also created a digital trust center in the Netherlands in order to help businesses increase their cybersecurity. And we developed a national system to facilitate the exchange of cybersecurity information. There is now a cybersecurity council and a cybersecurity alliance where public bodies, private organizations, and the research
community work together to make strategic and practical improvements to cybersecurity in our country.

But public-private partnerships alone won’t be enough to respond to the ever-mounting threats. And when it comes to addressing security concerns, we must find a new balance because security can no longer be an afterthought. Remember what I said, it’s not if it’s going to happen, it’s about when a disruption is going to happen. As a government, we must act earlier and more assertively in the situation where a crisis or an incident would occur. And maybe even more importantly, again, work together with all the other stakeholders to be prepared as well as possible.

I told you before, the Netherlands has an internationally crucial digital infrastructure. That means that whatever we do, we cannot look at it, isolate it at a national level. We need international cooperation. Together with several partners such as the EU, we took a number of steps to keep up and become more resilient. However, due to the rapidly doesn’t describe it – the incredibly fast technological developments, and on the other hand the transboundary risks and threats, it is necessary to take the next step in international cooperation, to increase security in the international digital domain. And you would have expected the Netherlands and the U.S. should work even more together.

We are already natural partners in that respect. And I witnessed that in the meetings I had during my stay here in Washington with the various agencies, but also the corporates related to cybersecurity. We are natural partners. As a Dutchman, I admire the American approach. Your approach to cybersecurity can lead as an example on how we can develop even further. For example, the way the Americans handle critical infrastructure and supply chain risk management illustrates the possibilities and necessity of a common approach and cooperation. And on the other hand, you are also the land of the free and the home of the brave.

Freedom, as well as fundamental rights, are in your DNA. And in my youth, I was much inspired – I know this is a long time ago, my youth – by Steve Miller. You – some of you may recall his song “Fly Like an Eagle,” which was about hope for the future. There’s a solution, was the recurring line. And you know what? They called him the space cowboy, always positive, searching for answers – and by the way, never on drugs. But that’s another thing. He did drink some whiskey. They called him the space cowboy. And I certainly would hope USA would be willing to take up the role as a future cyberspace cowboy.

We need the USA if we want fruitful international progress on cyber. And as I said, it will only be possible to enhance cybersecurity through international cooperation and international legislation. We are a relatively small country, you all must know, although I’m proud to say we’re 30 times bigger than your smallest state, Rhode Island. On Waldseemüller’s map – that’s a consolation for those of you who are disappointed that he gave the name America to Latin America – we, the Netherlands, were not even named on that map. We were then just a collection of low countries by the sea.
But that sea, the threats and possibilities of all that water and us being below sea level, learned us to cooperate with public and private partners and with people from the most difficult religions and backgrounds, with an especially strong reputation in the maritime. It was not difficult to also ensure that in the maritime cybersecurity. And maritime cybersecurity sets a good example of the cooperation between our two countries. In this area, U.S. and Netherlands took the first step in creating a partnership. And we’ve got many shared interests when it comes to maritime cybersecurity. Creating a synergy in this sector by sharing information and best practices is the only way to keep our ships and ports digitally safe. And I’m very pleased to see that now other countries are joining the two of us in the cooperation – like Denmark, Germany, France, and U.K.

So whether on land or sea, cyberspace is a world we are still exploring, a world we have to map out, define, regulate. But there’s still plenty of dragons at the end and at the edges of the map. We have the tradition in slaying those dragons lots of explorers, adventurers, and cartographers in our history to be proud of.

But finally, OK, I must admit we just missed out on discovering America first. But we were the first to discover Australia – not bad – long before James Cook sailed along. And a Dutch cartographer, Adrian Bloch, was in 1614 the first European to draw a map of your East Coast, with the island of Manhattan – or New Netherlands, as it became known to him. And OK, we should never have sold New York, but what can you do? People make mistakes, right? And as they say, failures achieved in the past offer no guarantees for future lessons learned, just as results achieved in the past offer no guarantee for the future.

So we should consider cyberspace as a whole new challenge – a challenge that is difficult to know, difficult to grasp, difficult to map, and where we must not fear to now and then fail and make a wrong turn or a wrong decision. We have to challenge, and we have to face it, this challenge, together – working together, talking together, like we’re all doing here in these days that I’m visiting. That’s a role we have to play if we want to take it further. And I’m really proud that we have such a great partnership on this with the U.S. and really looking forward to take the next steps.

Thank you very much.

Catherine Lotrionte: OK. Minister, before you take questions, I’m going to get a mic from someone and – but I think you can hear me.

I’m going to – can I ask a quick question before I hand it over to everyone?

Ferdinand Grapperhaus: Sure

Catherine Lotrionte: So I understand that when your prime minister visited the country and met with President Trump that they entered into an agreement that they would form a partnership, the Netherlands and the U.S., to work on cyber issues, challenges. So I’m wondering, from your perspective, could you add
anything to that general description about what that might mean? And particularly, where might you see the priorities? There’s a lot of challenges. Cyber, described broadly, can cover a lot of different things, some of which you’ve talked about today. But what do you think the priorities should be or are in that partnership? And can the Netherlands and the U.S. uniquely working together kind of internationally make a difference?

**Ferdinand Grapperhaus:** I think we can. I think the biggest priorities are awareness, resilience, and risk management.

Now, risk management is something that we as governments with experts corporate companies, you know, expert in cybersecurity, we can take upon us. So let’s not spend too much time on this. I would always invite other stakeholders, such as institutions, civil liberties organizations, everyone who has a stake in this issue to join us on that. But I’m not so – I don’t have great concerns that we can’t get there when it relates to risk management.

Going back to resilience, resilience is only possible if awareness is created. If you have the awareness, then, again, resilience is something I think we can solve, again, together, and I won’t go into detail. I think I already made some observations on that.

So I come back to this issue of awareness. And just one anecdote. When this report came out in the end of August of one of the most distinguished advisory councils, the Scientific Advisory Council in the Netherlands, where they – the quintessential conclusion was it is not if a cyber crisis will happen at a certain point, it’s only when, there was hardly any media coverage of that, let alone a shockwave going through society. And that – getting the public, but also getting the opinion leaders, everyone aware that cybersecurity, in fact, means it’s not a given that our cyberspace and our digital world work every day and every minute, it’s something we have to keep an eye on. So awareness is a really very important issue. And by the way, also awareness against cybercrime, which is kind of low with the public and even with corporate companies, and awareness of cyber threats as well. So that we have to work on a lot, I think.

**Catherine Lotrionte:** Thank you. William will give you the mic. If you could just introduce yourself and tell us where you’re from.

**Lin Shenko:** Hi, everyone. Thank you for the sharing, sir. So my name is Lin Shenko. I’m a current graduate student from Johns Hopkins University studying engineering and international studies.

So my first question is, I just learned something new from the gentleman who sit next to me. Like, people are talking about the cybercrime issues, like, even before I was born 25 years ago. So compared to 25 years ago, what is, you know, like, poses the biggest change in terms of the issue? And right now, when we human being are facing, you know, the ever-accelerating of the technologies, like the 5G communication technologies and, you know, encryption technologies like blockchain, so how can we actually, you know, make these efforts and progress to keep up with the advance of the technology?
And second question, very quick, is you mentioned, like, government should take the lead while collaborating with private industries, and while raising awareness would be the biggest challenge. So I wonder, like, what would be your strategy, like grand strategy? Would you like to be doing something more like bottom up or top down, you know, to address those issues and challenges? Thank you.

Ferdinand Grapperhaus: OK. You don’t mind that I more or less divide your first question into A and B? OK, which is not a very digital way to approach it, but anyhow.

So the 1A question is, indeed, cybercrime is with us for some time, so how do you relate to that and what is the - how has it developed, and what are we facing, and what are we doing about it? I think cybercrime, indeed, has swiftly developed in the past five years. We see that in statistics and we see that also in police reports. And I think we should admit, as governments and law enforcement authorities in many countries, that we were a bit slow in starting up against that. And in the past, well, let’s say four or five years what I’ve seen is that law enforcement in many countries have picked up on it much more. There’s more investment in knowledge with law enforcement people, that they know what it is about, what they’re dealing with, what the measures could be to go against it. And also from the government perspective there have been more campaigns towards the public to watch out for cybercrime.

We’re still not there. And I think – and that is more or less your B, 1B – we must realize that it becomes very, very sophisticated, and with that sophistication it won’t so much help that our law enforcement has become much more sophisticated on cybercrime. You must take the public with you. And here again I come with my more or less chorus of the song, which is awareness, awareness, awareness, because people cannot survive on the internet digitally if they don’t have a certain amount of certainty against these activities. So we have – here there’s a responsibility for me as minister of justice and security, but also for other people in my Cabinet to make especially vulnerable groups like elderly people, like people who are less digitalized, aware of these threats.

Number two, I think we must realize that what is coming to us, the strategic challenges on cyberspace relate very much to, indeed, create a(n) ideal world of cybersecurity which – not a guaranteed, 100 percent, waterproof, safe cyberspace, but to really get cybersecurity to the maximum, which it is not now. I’ll tell you – I’ll make you a small confession. So my country is much depending on dikes and dunes, and the systems there are also very much digitalized. And I must admit that last year we found out that part of the system is still running on 2G. I mean, for the elderly here, I would say do you remember 2G? And there our strategy must aim at getting everyone – also the companies that provide IoT products, for instance, or services – everyone into not only awareness, but also an active role on cybersecurity.

And on the other hand – and this is what I said in my lecture – it’s a challenge, but it’s a necessary challenge we must meet to develop our own cyber capabilities as well. And I’m honest about that. We are very cyber-
minded. But we need the U.S., for instance, and we need other countries to develop that together.

I think I did 1A and B, and 2.


I had a question about the balance issue that you raised with regards to encryption being a blessing and a curse. Why couldn’t the balance be established between full end-to-end encryption and law enforcement hacking, for example? Is there anything that government hackers, you know, need more, or that they can’t accomplish that they need to weaken encryption in order to accomplish that?

Ferdinand Grapperhaus: Well, first of all, I think if you want to reach a balance in a problem, then it’s foremost that everyone who has a stake in the problem is involved in finding the solution. And you know those situations at school or at university, you were into a conflict and there was a mediator and five parties were involved in solving the issue, and you were not involved, and you come up and you say, well, hey, where is my stake in the solution? So we need to do that with the tech companies, with the civil liberties organizations with law enforcement agencies, and with the governments responsible for cyberspace. That’s number one.

And number two, standing here today I don’t know the end solution of the equation. I will admit that to you. And why is that? Because I need to know, you know, what are the exact details/interests of all concerned, and how can we then – and we need experts on that – how can we balance them in the right way. But let me assure you I’m not a back-door man. I think you know what I mean. I think we have to solve this. If we solve this in the right way, we have to look each other in the eye and find let’s call it a front-door solution. That’s the only way that it’ll work.

But I hope you do realize my problem is not so much that we have all types of communication that have encryption or end-to-end encryption. I mean, in the old days – that was when I was at school; I’m sorry for those of you who weren’t there in those days – but in the old days, you had a – you had the right to the secret of the letter. And when I posted a letter to my grandma, I can assure you there was no sensitive state secrets in those letters, but I sealed the letter and no one was allowed to open that letter. So this is of old times, end-to-end encryption. It’s also from the analog world, and we must respect that. My issue is not so much that.

My issue is that in the old days the old mail letters were not massively used for communicating these horrible – and I really – I am telling this everywhere – this horrendous type of child pornography, child exploitation, and what have you. And this is one of the – one of the flaws of internet. It has brought an ideal communication for this kind of crime. And I want to solve it, and I want the help of other stakeholders. I don’t want to sit in a table, everyone sitting like this and saying I have my interest, get out of my room.
There’s a gentleman – oh, sorry. I’m sort of an auctioneer telling you who to

Geoff Odlum: Thank you, Minister. My name is Geoff Odlum.

I’m a recently retired State Department Foreign Service officer, diplomat, so I’m particularly interested in hearing a little bit more about your vision for what effective international cooperation and international – I think you said international legislation or regulations would look like, and the role for example of international bodies like Europol or Interpol or the U.N. agencies who do law enforcement like UNICRI or UNODC. What role should they play in helping set global standards and enforce global standards? Or do you see it being – continuing to be a bilateral and nation-state function? Thank you.

Ferdinand Grapperhaus: Well, I would certainly, sir, prefer solutions that have global standards with possibly a sort of a band for specific geographically-defined situations, OK? But I’ve seen how Europol has really developed the crimefighting and law enforcement in the EU in a positive way, taking with it in a positive way human rights in respect to law enforcement. So I’m very much an evangelist of those kind of cooperations, bringing us towards global standards. And it was your compatriot, Carnegie, who in – I always forget – it was – which year was it, 1905? I forget; I’m sorry – who initiated the Peace Palace in The Hague and already had this vision of, you know, getting these types of issues more on a globalized basis.

And we’re not talking today about war crimes, but I think the Nuremberg trial was a gigantic breakthrough. A lot of people don’t realize that. Before the Nuremburg Trial – and we thank that to two Jewish professors, one from Lviv in Ukraine and the other from the United States, I think from Boston. And they invented the whole concept of genocide and were the architects of the Nuremburg Trial. And you know, it’s – you cannot – almost not any more imagine a world before that. So when we talk about cyberspace we need those kind of internationalized standards so we can – I think if we have that, we can have a massive – make a massive mileage in the whole subject.

Catherine Lotrionte: We’re going to have to –

Ferdinand Grapperhaus: Yes, but one more gentleman is already with his hands in the air for an hour. So I mean, let’s reward him.

Sean Lyngaas: Hi, Mr. Minister. Sean Lyngaas with CyberScoop.

I’m wondering – you know, you said you’re not a backdoor man, but how is this time going to be different in terms of a search for a technical solution to, you know, so-called going dark? Every expert I talk to says that you can’t really accomplish what you’re trying to accomplish without subverting security controls and making the internet less safe for a lot of people. So what technical experts are you talking to in your search for an answer to the going dark challenge?
Ferdinand Grapperhaus: Yeah, you mean how to get to a solution which creates the balance we discussed before?

Sean Lyngaas: Yeah. Because it’s been tried many times by law enforcement. And every cryptographic expert says that it’s problematic because –

Ferdinand Grapperhaus: No, it is – it is problematic. But you know, the reason that I am stressing the urgency of this discussion, that I – let’s say I understand that your attorney general has with his letter of beginning of November brought forth this urgency, because the expansion of – and I’m talking about heinous crimes. I’m not talking about phishing mills or whatever, OK? I’m talking about in the things like child exploitation, et cetera, through internet. Well, in my country – and I spoke to the experts here in the U.S. in the past days, it’s the same there, it has grown exponentially in a shocking manner. And we – so what I’m bringing into the situation is not that I’ve decided who’s going to make the technical solution. I don’t have the arrogance even to think that I can bring that forth. We must try to find a working compromise and I don’t have the solution now. But the only thing I’m bringing in is this problem is growing so much out of hand. You know, when I was in my 20s, child pornography and everything around it was – man, it was to be found where? In some dark alley or whatever.

It was – you couldn’t get to it, if you know what I mean. It was really a problem that the law enforcement agencies, they attended to it and it was horrible and it happened – child abductions and whatever. But it was – well, it was an overseeable societal issue and these days it is – I’m making this alarming statement – it is going way beyond this.

And you may have noticed I’m not talking about things such as hate speech, for instance, because I find there already you have a component of freedom of speech, whether you like it or not, and then the discussions become far more hazy. I’m talking specifically about this issue.

And you know what? The big internet companies, when it came to this roundtable everyone agreed that freedom of speech or any other fundamental right is not at stake in this situation. Everyone agrees to that, that people who are involved in this have more or less rejected their own fundamental rights to freedom of speech or whatever.

But, again, so I hope I don’t disappoint you. I don’t have a ready answer how we are going to do this technically. The only urgency I bring to the discussion table with stakeholders is, people, we must now discuss it. In America, I think Messenger is much bigger than WhatsApp and Instagram. OK. In the Netherlands, Instagram is vastly popular. WhatsApp, even more.

Our police have, through other ways because they were given access to telephones, found out that chat boxes of WhatsApp that is already end-to-end encrypted in the Netherlands have enormous – that there are chat boxes with enormous exchanges of child pornographic material with children being offered to people for a price, et cetera.
And I went over to the NCMEC, the National Center for the – Missing and Exploited Children. Sorry. And they had statistics for the U.S. and for my country of what was reported by the various social media. Until now, Facebook has reported a lot of this stuff going through Messenger because it doesn’t have end-to-end encryption yet. In the Netherlands, WhatsApp, the number is like this of reports. Why? Because end-to-end encryption makes it impossible to get there.

So I stand here saying – and maybe that is a slightly different tone from the letter your attorney general sent. I don’t know. But I think we share the same view. We must have a roundtable discussion, sit with each other saying how are we going to deal with this problem.

So I hope you understand that is my problem and not so much the problem how will end-to-end encryption, in the end, go further because I think end-to-end encryption is a – well, it’s a technical fact of life.

OK.

Catherine Lotrionte: Sir, thank you very much. I’d like to thank you. Thank you again, Minister.

(END)