SEMINAR REPORT

June 2024

ISC Special Lecture

"International Law and Emerging Technologies"

by Professor (Emeritus) Vitit Muntarbhorn
Organised by International Studies Center

5 September 2023
Narathip Auditorium,
Ministry of Foreign Affairs

SEMINAR REPORT

ISC Special Lecture

"International Law and Emerging Technologies"

by Professor (Emeritus) Vitit Muntarbhorn

Organised by International Studies Center

5 September 2023

Narathip Auditorium, Ministry of Foreign Affairs

INTERNATIONAL STUDIES CENTER

ISC Special Lecture

International Law and Emerging Technologies

Publisher

Printed in May 2024 (200 copies) by International Studies Center,

Ministry of Foreign Affairs, Bangkok

E-mail: isc@mfa.go.th

Printing

P. Press, 129 Sukhumvit 81, On-nut, Suan Luang, Bangkok 10250

Tel. 02 742 4754

Publications of the International Studies Center are available for download at isc.mfa.go.th

---

National Library of Thailand Cataloging in Publication Data

ISC Special Lecture “International Law and Emerging Technologies”.

-- Bangkok: International Studies Center, Ministry of Foreign Affairs,

2024. 38 p.

1. International law. 2. Technology. I. Title.

341

ISBN 978-616-341-146-4

ISC Special Lecture

"International Law and Emerging Technologies"

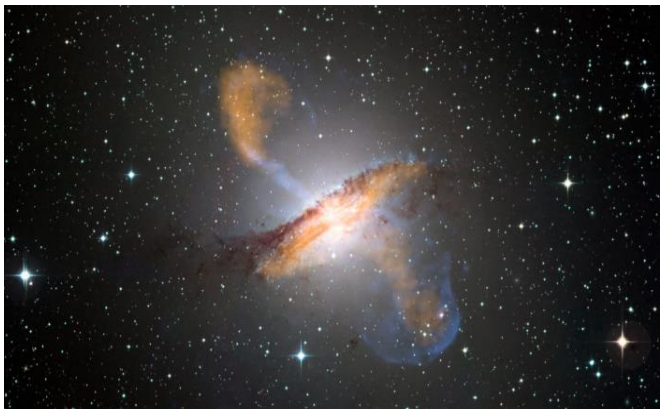
Professor (Emeritus) Vitit Muntarbhorn
Faculty of Law, Chulalongkorn University

Good afternoon, my dear friends and family. Thank you very much for coming. This is like a family gathering. So, a warm welcome, and we are here really to celebrate the 36th anniversary of the International Studies Center (ISC). Let's give the Centre and everybody a warm applause.

I hope you all have a relaxed afternoon with me. I will choose six main issues to be dealt with in terms of technology. Then, we will have a discussion period. Finally, if there is time at the end, there are two case studies that I can also use.

First of all, let me thank the ISC for inviting me here, Dr. Tej Bunnag, Chairperson of the ISC Advisory Board, Dr. Anuson Chinvanno, Director of ISC, all friends and relatives who are here, including the Faculty of Law, Chulalongkorn University and others who are with us and online.

The talking point is international law and emerging technologies, but I'd like us to reflect for five seconds. What is your image of technology in terms of the visibility of something very prominent in your mind? Have a think for five seconds. I will show you what I think is my image of technology.



Source: Independent[1]

This is my image. What is it? The telescopes enable us to see this fascinating image, but it has been there in our minds since ancient astronomers, centuries ago, but more recently visible.

[1] https://www.independent.co.uk/space/how-to-see-andromeda-galaxy-stargazing-astronomy-science-space-a8562766.html

This is the Andromeda Galaxy, and what is Andromeda going to do to us in three billion years? Andromeda will collide with our Milky Way, and I think this is one of the most fascinating technological studies stories for me as a learner and as a student.

It will collide with the Milky Way, and we do not know what we are going to call it, actually, "Andromeda?", "Milkomeda?". Today, it is about semantics and the logic of technology as well. If you look around, you will see a blue around the halo. It is a spiral galaxy, and what is the meaning of blue rather than red in this country of no colours? The blue means that it's coming to us. There is a gravitational pull. If it is red, then it is going away into the universe. But if you look hard and fast, a sort of blue enables us to see that gravitational pull enabling Andromeda to come towards us, and we will meet in about two billion years.

At the moment, it's about 2. 5 billion light years away from us. And according to technology, we know the speed of this blue coming to us. It is about three hundred kilometres per second, coming to us gradually. That is an absolutely mind-blowing personal experience that is very educational and enables me to be self-reflective as well on technology, telescopes, the Hubble, the web. The philosopher, the astronomer, etc. centuries ago from Asia identified this phenomenon, which is actually a spiral galaxy coming towards us, and we will collide and merge somehow. That is two to three billion years from now.

Today, I will try to reduce some concepts, laws, to a very simple understanding of both international law and technologies. When I humbly use the word "international law", I mean a system of rules above the nation-state, above us, some sort of regulatory system up there, transcending the state and other actors.

When we look and see the evidence of what it is, when you talk about law, you are really talking about something enforceable. The legal word is "binding", and the evidence of this legal framework is through certain elements such as treaties, agreements, conventions, and customs which can be binding rules through usage. For example, even if we do not have a written law, we can say, "torture" is forbidden in the practice of humanity. I think that is a custom that we all accept, even though we might not have a law, and Thailand has a new law on this now as a manifestation of that custom, but it was always part of international law long ago, even though there are breaches.

General principles of law maybe something slightly moral, for example, the principle that in war, civilians should not be attacked. That is known as the principle of distinction. As for other sources of international law, these cover jurisprudence, namely, cases, legal decisions, and the World Court. The World Court is famous for Thailand in regard to a certain case pertaining to Thailand. A key case now before the World Court in The Hague has to do with climate change, seeking advice on climate change as to whether we have certain rules that enable us to do certain things and our responsibility towards not only us but also the next generation.

We are waiting for advice on an intergenerational perspective of law now from The Hague. That will count as part of global jurisprudence through local and international courts. In addition, we sometimes use the word "doctrine", which is the writings of publicists, another source of international law. Maybe what you write is or can become part of international law, guiding the

world community on the preferred options, the preferred way to respect common humanity as well as nature.

Importantly, the way we measure international law is not only through those elements but also through what we call State Practice—what you, the diplomats, send to Geneva and New York, how the foreign ministry and others communicate with each other. Everybody says torture should be forbidden according to communiques, press statements, NGOs, etc., but particularly between states. That is of some weight.

We will see that the gestation of the rules is now taking place in a great state of flux because technology is in a state of flux. With that in mind, the UN is not far. The international community is not far; another word you will hear along the way is "hard law".

Hard law means the type of rules that are enforceable, that pressure for some accountability, maybe sanctions locally or internationally. Those are rules pertaining to hard law. Like the Convention on the Rights of the Child—no child should be punished by the death penalty. That's pretty well hard law and also applied in the nation-states. At the local level, hard law means legislation, acts of parliament, and statutory law through parliament.

Then, you will hear the word "soft law", which means policies, guiding principles, and the most famous soft law that is almost hard is Sustainable Development Goals (SDGs), which also pertain to us. SDGs guide the world community in terms of preferred development for the future.

As for Resolutions/declarations in the UN, of the UN—I have to work with Resolutions all the time in my humble role with the UN. Resolutions are not binding. They are neither treaties nor conventions, but they might have elements of custom which could bind, but generally the Resolutions are mere recommendations, something softer. Then, there is the mixture of both, sometimes I say hard and soft, you get this when you look at this spectrum. You might have a convention or treaty, but the rules inside are quite soft, and there is not much of a sanction. Thus, there can be a bit of a mix between the framework of the law and what is slightly more flexible inside that law, a treaty or local legislation.

The word "regulations", as used by my humble self and others, will also mean hard law. Under the state, regulations could also mean statutory law and more, and in regard to the international perspective, of course, regulations pertain particularly to the hard law of international treaties and conventions.

Self-regulation, which is a very dominant phrase in this discussion, is about industry rules of conduct—how your digital industry comes out with a code saying, "Okay, we will be careful about children", with some self-monitoring and leveraging between industry, not necessarily touched upon by the state but left as a code to be operationalised and pressured, leveraged through the industry, through the business sector itself.

The other word which is probably new to you is "co-regulation". Now, this is very interesting. You might have self-regulation through the industry that is also supported by the state or shared monitoring between the state and the business sector and stakeholders. A very famous case—anybody from Belgium here? The famous case of self-regulation on digitalisation that you

will hear about is on Cloud self-regulation in Belgium, which is a code of ethics to respect your personal data in Belgium but also backed by the state.

It is bridging between hard law and soft law, as well as by the European Commission as a regional body up there. It is a very good example of how we can cooperate. International law provides room for cooperation as well as a sense of responsibility along the way. You will hear different shades of both along the way.

The word "technology" is about scientific knowledge leading to a practical outcome—maybe a product, a service, or a creation. The most famous today is ChatGPT, and if you have not tried it, try it and believe it or not. The term "emerging technologies" is used to cover new tech or older tech with great potential for expansion, for example, neurotechnology. Another very attractive phrase "frontier technology" is implying something cutting-edge, something new and pertinent. Today, if you ask me to do a listing of technologies, this is the UN's latest listing from the UN Conference on Trade and Development (UNCTAD) 2023. Seventeen frontier technologies can be sampled below, including Artificial Intelligence (AI).

The samples are the following. You might see in an article from the newspapers an item about **the Internet of Things**, where the internet can be connected to many things, your shoes, your bedsheet. There is also **Big Data**, not small but mega data, and this is very important issue because it is collected by mega-firms and sometimes also abused by mega-firms, mega-platforms.

Blockchain means technology that can share data and information; there is a coalescing of various partners there. **5G**, everybody knows it a little bit in terms of your mobile but very connected in terms of technology that's very much at hand, particularly your mobile. **3D printing**—three-dimensional printing that can help you construct. **Robotics**, which I will merge with AI, and the famous robot—you know, it looks a bit human, but it is not. There's a famous book by a Nobel laureate called "Klara and the Sun", which, if you have not read it, is very incisive regarding how we merge our love and relationship with non-humans, at least through literature. **Drones**—in the news every day, the attacks over there, over here. Europe is a witness to this every day in terms of drones in a nearby conflict area. **Gene editing**, whereby your genes might be edited so that genetically you will be improved, and the question is: are we playing with Frankenstein or not? **Nanotech**, which is small tech, usually medical and usually running inside you, and we'll come to that maybe later. **Solar PV**—solar cells, panels that we wish to see more, but be careful where they are coming from, and what about the minerals behind or what about the elements behind the cells. There is then the **Concentrated Solar Power**, **Biofuels**, **Biomass and Biogas** to do with bio waste, and the like that can generate some energy, which can be renewable. **Wind Energy, Green Hydrogen**—the cleaner one, as compared with carbon, and we'll deal with that in a moment. **Electric vehicles (EVs)**, but do not forget EV batteries (EVB) because the crunch today is EVB, which is the batteries and the implications of technology for Law and the environment. That is the spread of technologies, according to UNCTAD.

In terms of the UN Human Rights Council in Geneva, this year it is dealing with "Four-tech". Some documents are available on the internet already.

One: **Military Tech**, particularly autonomous weapons and killer Robots. How do we deal with them?

Two: **Neuro Tech**, fascinating. Maybe insertion here instructing my hand to move through the neuro vibe.

Three: **Cyber bully**, bully on the Cyber. It is linked with, on the one hand, freedom of expression and, on the other hand, privacy. Not to be attacked by hate speech, disinformation, or misinformation. I will deal mainly with those three here because I have another list that interests me, and I want to share with you.

Four: **Climate Change tech**, related to green technology.

For me, there is an additional other list:

Biotech, such as genetics.

Cybercrimes, I should deal with that a little bit because all these countries have new laws on cyber security, including this country. Do not forget the Computer Crimes Act, which is also very famous. How do we deal with cybercrimes? Through more laws?

Finally, **digitalisation**, including references to avatars and all the Meta stuff and **Artificial Intelligence, including Robotics**. We will see what timing we have to deal with those.

First, let's have a look at military tech, **Killer Robots.** What is the state of international law on this, and how do we deal with it? Do we prohibit it, or do we regulate it, and what is the channel?

We fear Killer Robots, especially if they are self-automated. If they decide themselves without human control, that is the fear. Today, there are two tracks internationally to deal with Killer Robots. One is traditional, expanding the traditional. The other one is new. The traditional one is to expand an existing treaty and expand an existing hard law in the form of a convention. The convention concerned is the 1980 Convention on Certain Conventional Weapons (CCW). Now, this is a funny convention. Why? Because if you want to join this convention, you must join at least two other mini-conventions out of five. Basically, the convention is a framework convention to deal with various weapons, but it gives you the choice of choosing two out of five other mini-conventions that are very specific and operational in terms of the weapons themselves. The tone of the whole framework is to prohibit absolutely or to regulate with conditions.

The five mini-ones from which you have to choose two out of five are these very quickly:

1. On non-detectable fragments of weapons: shooting at you, and you cannot detect the fragments within you.
2. Incendiary weapons: fire, burning.
3. Booby traps and certain types of mines.
4. Blinding laser weapons.
5. Explosive Remnants of War: everything that is not exploded, excluding mines. Little bombs in the trees or so on are explosive remnants of war.

If you join CCW, you must sign up for at least two out of those five. Countries in Southeast Asia, which are parties to this convention, are few and far. The Philippines, Cambodia, and Lao PDR have experiences on this front in terms of being parties to CCW. That is one track, but there is also power play. Never believe that law is this law alone; there is always a power play and international politics behind who controls the whole process.

That is why you have another track whereby the power play wants to have a different treaty, not the old one, but a new one. So, they are now also negotiating a new treaty on autonomous weapons. The concerns that we bear in mind include the right to life, the fear of indiscriminate attacks, the robot decides by itself to attack people, and the lack of humans in control, that is the fear. The other track is to have a totally new treaty which interweaves also with the power play by very superpowers, irrespective of the old CCW.

The latest advice from the intergovernmental expert group linked with the UN and the CCW is to emphasise elements of law, which are actually very simple elements both in terms of the old custom-usage accepted principles of a certain enforceable nature, as well as logic. It is basic principles. The group this year said that whatever we have in terms of innovative treaties, maybe a new protocol, or a new Mini treaty to add this to the existing CCW, we must highlight the old war-related principle of distinction. You cannot attack civilians; you can only attack the military. That is the principle of distinction. You must prove military necessity if you are going to carry out the attack in regard to a military targeting, as well as proportionality to ensure that the military advantage is not excessive and does not outweigh protection for people, does not cause too much collateral damage, and there is a backbone in terms of traditional established warfare-related law known as international humanitarian law, as well as various principles in the various Red Cross Geneva Conventions. Some of the representatives of the Red Cross movement are also here to testify to that.

Which way do we go? We are not quite sure which power controls which track, but anyway, I think that with autonomous weapons, particularly Killer Robots, at least you must have some regulation, at least you must have some monitoring, and if there are violations like killing civilians, for example, some responsibility and accountability to be aired and discussed in the negotiations.

Neurotechnology. Now, this is very interesting because it's about the brain-computer interface or the brain and the robot interface. Nobody denies the medical benefits, particularly perhaps for dealing with Parkinson's disease. But there are human rights and international law concerns, including what about it being a threat to health, maybe rather than being helpful to health? What about the misuse of the tech for human experimentation? The UN paper on this issue is still gestating and gelling, and there are concerns in regard to what some call neural rights as new rights. But I would say actually, we're just talking about established human rights, established international law, but expanding the leverage to cover neural issues, including mental privacy. I want to keep what is inside private rather than leaking it through neural waves to the robot in my hand. There is the issue of cognitive liberty, the way that I build my knowledge. I don't want to be manipulated by the contraption, and there is then the mental integrity, as well as psychological continuity as a human being.

The fear is that some people want a neural augmentation that might lead to a super-intelligent person, maybe a *hubot*, ultimately beyond the robot. Additionally, in terms of testing at the local level, we also differentiate between invasive neurotech and noninvasive neurotech. Invasive neurotech means inserting something into your inside - the brain or the cranial area. Noninvasive means something outside, but which operationalises your neural wave towards the contraption outside.

Today, through experimentation, what is now increasingly allowed is non-invasive neurotech; it is now being used particularly to help persons with disabilities, for example, a headset to help someone who is with a disability that can order the hand to move. But the big question, subject to experimentation today, is invasive neurotech, and that is still being tested in one big developed country, and the rules are still unclear at this point in time. Traditional rules come into play in terms of respect for privacy and respect for physical and mental integrity that can be expanded to cover the neural spectrum.

The trials are taking place, and interestingly, one big company that invests in EVs and satellites is investing in neurotech. So you do not have to look very far for the commercial implications of all this. Maybe we should really think hard about emphasising more the medical, therapeutic, and diagnostic side, rather than consumerism to go for the Uber person, which might ultimately be negative.

The puzzle from neurotech is a puzzle pertaining to a lot of technologies. I think because it is a recurrent puzzle, it is good to test this with every technology we are looking at, maybe the 17 that was listed earlier. One is safety. Two, security: is it secure, and whose security is it? Is it my security, or is it the state security because a lot of the tech is being used by the state to monitor, famously, the cameras? Three, the equity factor, poor or rich, online or offline during COVID-19. I was online, but think of a lot of kids, children who were not online at all. Inequitable, in terms of dispersed availability of tech. Four, equality, in terms of non-discrimination. What about tech that is used to discriminate and profile? And five, privacy: it is about my privacy in terms of data, but privacy is also tested by exceptions. The right to privacy is not absolute. National Security can creep in on me even if I claim my right to privacy.

Emerging issues on this front include: do we go for a diagnostic-therapeutic versus consumerism? Do we go for prohibition, hard law, or regulation with conditions - hard law - or free market, maybe with a bit of soft law, self-regulation, or co-regulation? What about responsibility? Ultimately, I think a very interesting offshoot in neurotech is: what sort of medical insurance are we going to build in the future? The big companies that get into this are wise enough to move on this front to ensure that they are covered in terms of liability, at least in civil claims. There will be different types of insurance systems as we get more and more into these intricate technologies, at least from the market system. But equally important is us, the people, the small people who also need to be insured by law and by other means against abusers.

Cyberbully. Being bullied, such as via hate speech on the internet, for example, is something very common, and it affects a lot of children. Yet, what you face is a dichotomy, a paradox between freedom of expression, on the one hand, to say, *"I don't like you"*, and freedom, the right to privacy, on the other hand, not to be attacked, at least unreasonably. The blending is

not an easy one. The lawyer might say you need more law, the lawyer will probably say that, but I would not trust it too much. I would twist it around by saying, why don't we look at cyberbullying from the angle of the need for an educated and empathetic, empathic, sympathetic population? A kind population can help to prevent cyberbully. Do not just trust the law; that is one entry point. If you need a law, then we have a standard. The international standard is you need a law in regard to incitement to hatred that can lead to violence or discrimination. It is a very high standard; incitement to hatred leading to discrimination or violence means: I provoke you to hate that person and do something nasty to that person, something very serious as a triangular relationship, rather than just saying, *"I don't like you."* The bilateral relation of *"I don't like you"* can be dealt with through other means rather than a stringent law.

Remember the abuses, particularly by non-democracies, especially where freedom of expression is impeded. Anyway, both freedoms, the right to privacy, and freedom of expression are not absolute. They can be constrained by national security, public health, and public morality. In international law, constraints on basic rights must pass and must prove that they abide by a three-part test as limitations on the limitations. If the government here, whatever elsewhere, wishes to constrain our freedom of expression, the government must prove that number one, the limitation of freedom of expression or limitation of privacy, is based on a clear, fair law, not just arbitrary discretion by the authorities. That is known as the principle of legality; the exception to freedom of expression and the exception to freedom of privacy must pass that test, number one.

Number two, the authorities must also prove that it is necessary to limit the right as well as proportionate, being proportionate to the risks. In other words, if it is a mini cyberbully, for example, on the internet, it is just not reasonable, necessary, or proportionate to enable the authorities to come crashing in and take all computers, some of which have nothing to do with the cyberbully. It is just not necessary or proportionate to the risks. The authorities must prove necessity and proportionality.

Thirdly, if you are to limit freedom of expression, even not "nice" freedom of expression or, on the other hand, freedom of privacy, the authorities must prove legitimacy. The ends must be legitimate, meaning maybe constraint on freedom of expression against cyberbullying, maybe constraint on privacy in regard to cyberbullying, because it is legitimate to protect the rights of other people, particularly children, rather than for arbitrary national authoritarian discretion, which is not a legitimate end. So, those are the three tests pertaining to how we can formulate a certain entry point to deal with both freedom of expression and privacy in regard to cyberbullying.

I will now jump to a very prominent issue today, which is climate change, and this is also an issue, one of four, being dealt with in Geneva at this point in time. A lot of it is about carbon reduction, and many of you are experts on that, but I will add something on green technology as well in terms of where we go with greener technology, particularly renewable, regenerative, and the like.

As you know, climate change is very much the agenda of the day, and part of it is about defossilisation, decarbonisation, and reducing carbon. The other side is adaptation to adapt our town and country to new conditions, to be prepared for natural disasters and so on. And today in

Southeast Asia, an emerging issue is where do we go with carbon tax? The lead country with the carbon tax is Singapore. Thailand is also contemplating this. But remember also that carbon tax is one entry point; it is not every entry point in terms of dealing with this. The other one is a very topical debate, carbon credit exchange, which is a voluntary phenomenon now whereby you can offset your carbon emission by buying carbon storage from another sector, particularly agriculture or forestry. Very interesting today that we are becoming more skeptical about carbon exchange even though it is around. Why? Because it may lead to greenwashing, not real reduction at all. We need to move towards a real reduction of emissions rather than just playing around with what is also very empirically difficult in terms of proving whether you can actually have credit for something that is very difficult to measure.

Another issue that has arrived is carbon capture; some advocate that they can remove carbon from the atmosphere through specific fans. The question is: where do you go with storing all that? The carbon sinks for storing all this are usually agriculture, or the oceans, or forestry, and there's a limit to all that. And who deals with it anyway? Big companies or small people who have very little say. A very important consideration among all this is to expand impact assessment, assess the possible impact on the environment, health, to human rights, and integrate it into risk management. This is based upon now a very well-known set of guiding principles, UN Guiding Principles on Business and Human Rights, which establishes the state's duty to have a framework to protect everybody. Very importantly, the business sector's duty to respect that framework by having impact assessments and risk mitigation, and finally, shared responsibility to remedy.

One very interesting situation now in the US is that young people in Montana took the state of Montana to court. The state of Montana refused to have an impact assessment in regard to its environmental law, and the young kids won. That is part of a harder law approach in terms of responsibility and accountability that comes into play also together now with the World Court judgment, or rather World Court advice on climate change obligations to the next generations coming very soon.

The quandary here is: please do not forget that every time we talk about the market, there is always a supply chain, the value chain around it, and then the economic power. With any market, you have those on the fringe, monopoly inviting demonopolisation and also SMEs that interplay with all this in terms of inclusion of just ordinary people in the discourse and the benefits from all this. The other side is technology, which can be greener. We have established by words in the UN a new right: everybody's right to a clean, healthy, and sustainable environment. That is by wording, but what does it really mean in real terms, in terms of rights and obligations? Mitigation, decarbonisation, adaptation, all those elements are there.

In real terms, if you test that new right from what is happening as a hub in this region, this region is going to become EV in EVB, and EVB will need some minerals. Traditionally, the problem was minerals from South America, lithium being used for batteries. For us, the next challenge is that we have a lot of deposits of nickel in this region, which can also be used for batteries. Therefore, it is important to bring into this impact assessment to prevent damage beforehand and assess the possibility of risk management.

Wind turbines and the like are very fashionable, also solar cells, but have a look and see who is impacted upon them. If you build wind turbines on traditional indigenous land, then you have a problem with the rights of indigenous communities. Likewise, even solar panels from this region, if you look hard and fast where they are from, they might be solar panels from, or the elements might come from a region that is actually very problematic in Asia, in a big country at this point in time. Please think around an approach that is empathetic around the emerging EV and EVB phenomenon, particularly the prevention of environmental harm in regard to the mining process.

I will jump to the other elements of note: cybercrimes and cybersecurity. Every country now has cybercrime-related law, and Thailand's cybersecurity law came out at the same time as the now famous "Personal Data Protection Law". Under Thailand's cybercrimes, cybersecurity law, if it is a very high-risk situation of cybersecurity, the national security people can impound your computer system without a court warrant. I would urge the authorities to be careful about that because whatever you do, it still has to fulfil the three-part test internationally of legality, necessity / proportionality, and legitimacy, and the approach to cybercrimes at the international level. While we do want to counter terror, be careful with who controls the whole process and be careful about the political setup of the country, the region, or whoever is controlling the drafting process of a hard law treaty.

Today, a cybercrime treaty, a multilateral cybercrime treaty, is being drafted, but there are dangers behind this drafting, including the power play. The most recent draft's problem is that data can be shared very easily between law enforcers of different countries on the basis of claimed cybersecurity and cybercrime without due regard for all the safeguards that we're talking about such as physical integrity, freedom of expression, right to privacy by everybody, and the various limits on state powers, including the principles of legality, necessity / proportionality, and legitimacy.

The legitimate ends can be law enforcement and people's benefits in terms of safety and security at large. So the preferred option for an international setting, as lessons learned for cybercrimes at the local level as well as cyber laws at the local level, is this: if we are to have a multilateral cybercrime, cybersecurity treaty, it must be very focused on particular crimes rather than being very expansive in terms of great discretion for the authorities to enumerate whatever they want as their preferred options vis-a-vis cybercrimes. The best example, I think, even Asian countries can agree to this, is the now well-known European convention on cybercrimes known as The Budapest Convention.

The approach of The Budapest Convention is a very specific approach to tackling very specific types of cybercrimes and not leaving too much discretion to the authorities to define the parameters of what they want to tackle. Budapest Convention says no fraud on the internet, no child pornography, no phishing, etc., rather than saying national security concerns. That is the preferred approach, and some Asian countries are also parties to The Budapest Convention, including Japan, Sri Lanka, and also the Philippines. Please have a look at that as a preferred option if the country is to have cybercrime, and cybersecurity-related laws.

I am afraid our Computer Crimes Act, which was originally targeted to phishing, sort of extracting information, is now a very largely implemented national law, in terms of national security, which is very much critically analysed internationally as a law needing reconfiguration.

Finally, let's have a look at digitalisation and artificial intelligence. Digitalisation can cover many things. A very famous aspect of digitalisation is the right to privacy, the "right to be forgotten". One day, this Spanish gentleman in Europe saw his information on the internet about his financial problems and potential bankruptcy, but later on, he cleared all that and yet that information was still on the internet, and he wanted it taken down because it was a breach of his personal data and situation. So, he sued and went upwards towards the European Court of Justice in Luxembourg and won. That was, and is, the origin of what we now know as the right to be forgotten. You have a right to ask the internet to take down your information, to erase it, rather than being there, especially if it is not true. This is the origin of the right to the internet that has crept into other countries, particularly to the European Union's General Data Protection Regulation, which has impacted upon this region very much. Southeast Asia has seven countries now with personal data protection laws influenced, rightly or wrongly, by European legislation.

A very important element is platforms; the internet industry needs our consent if our data are to be revealed and stocked. We are the data subject. Those who have, who must be careful are the data controller and the data processor. Maybe the companies or maybe the ministries will also need a check and balance in terms of a data protection officer. Thailand has been dealing with this now in terms of delegated (smaller) legislation on which type of data protection officer for which sector of the community, e.g. banking medical, security. Very importantly, there is the need for some due diligence to check or to test whether it impacts upon people's lives, privacy, and basic rights. The fines in Europe have been enormous, 4% of the year's income of the big companies, well, the mega ones you know about. Some of you will be interested to know that the new law in Europe also impacts us; the EU Digital Services Act 2023 is now implemented.

Interestingly, the Digital Services Act is more geared to protecting children from being targeted, especially by advertisements, and also to move towards transparency of the algorithm. The algorithm is the set of digital instructions impacting on us, through data being targeted to us in terms of various preferences. US laws are also emerging regarding a claimed right of access to the algorithm, to know that it is there and what it is about, to know how it profiles, and to remedy. This is linked with AI in a moment.

Thailand's law is now in full swing, but I would say that the other law is equally important: protecting my personal data on the basis of my consent. But be very careful; it is also subject to limitations such as national security, and some of the new legislation, the little ones coming out, are now to exempt the authorities from the obligation to respect my data. Therefore, I would also emphasise the need to concretise access to public information law, which we have. I want to know what you in the ministries, my friends, are harbouring in terms of data beyond my own data, as well as a check and balance.

The puzzle is: we are still living with the old computers or my old mobile; the new ones will come one day, particularly under Quantum Computing and the synergy created by Quantum

Computing and all the data and everything through their so-called qubits. The process is known as a very, very sexy term, entanglement, but will it break your encryption? Please be careful; nothing is secret on the internet. Ultimately, no anonymity.

Finally, AI, we now have a multilateral framework, but it is soft law. UNESCO's recommendation on the AI that came out in 2021 was hinting at the right to privacy, basic protections, and do no harm, proportionality in terms of what the state should do. Very general sort of ethical guidelines, no real sanction, plus it is a recommendation anyway, but it provides an ethical framework. For the lawyer, we are debating on whether you need a soft law approach or a harder law approach, and the harder law approach actually, is now seen again in the European Union. I am not flagging the European Union on everything, but these issues are very much seeping from Europe to other regions, and we need to be critically analytical and aware of all the good and not-so-good implications.

The European AI Act is on the verge of being passed; it has passed the vetting by the European Parliament already, and now it has to go through the Council of the organization. It takes a hard approach with this segmentation: number one element, prohibited AI, I'll come back to it; number two element, high-risk AI; and number three element, other AI. And AI, meaning today, particularly creative AI, generative AI, such as ChatGPT, and big companies also interplaying with lots of legislation, as well as litigation in Europe.

The prohibited AI includes subliminal AI, which plays with your emotions and activates the psychography, the psychology of children to be violent. That subliminal AI manipulating emotions is prohibited. The AI that profiles you and classifies your data to ensure that the state knows whether you are trustworthy or not; it is a social scoring or social profile, and this is also prohibited. The social score or social profile is already used extensively in Asia. So please be careful; it will be prohibited in Europe with trans-frontier applications. Some types of remote biometrics, facial recognition far away, not the close ones at the immigration, but when you are out there on the streets protesting, are forbidden, while others fall into the second category below needing safeguards.

The second category is high-risk AI, which includes law enforcement-related remote biometrics and that needs various so-called guardrails in terms of due diligence tests, assessment, and risk mitigation to ensure that people's livelihood safety is guaranteed, as well as their rights, subject to notification to a national agency and overseen by a regional body with also very heavy sanctions for violations. The latest implementation of the European Digital Services Act can now punish through sanctions vis-a-vis 6% of your global earnings if you are in breach of EU law, and that is a lot of billions.

Another front is the Council of Europe, which is another body and it is working on a more general treaty of hard-soft approach. Interestingly, ASEAN is planning an AI plan by next year. As a guess, ASEAN will work towards a facilitative approach of wanting more AI for ASEAN to be the lead region, rather than a hard law approach of regulation and prohibition. But be careful because there are implications - because some Asian countries are still waiting for democratic space. One big Asian country has now moved towards a regulation on algorithm registry to make

algorithm(s) transparent because algorithm (s) can also be biased, as well as the data sets that are used to train AI. The robot has to learn, but the data for training might be unfair. For example, if it is genetic data, the global genetic data spectrum is usually genetic data of Europeans and North Americans rather than Africans or Asians, thus it is going to be biased already in terms of genetic data. So, be careful. The algorithm itself might also be biased in terms of the sets of the equation or formula directed against or vis-a-vis one group or another.

Another regulation of this big country in Asia is against deep fakes in terms of deceptive AI. Be very careful with your voices now on the computer on your mobiles; they can be recorded or twisted. And even in the newspapers today, some bankers were tricked into believing the voices of their customers as deep fake. In this country, there is already a regulation against deep fakes, including hallucinations that can be generated through this new deceptive technology.

The draft Thai law on AI actually follows Europe a little bit in terms of prohibitions in regard to social scoring. I am interested in other aspects. I want to know whether it is the robots deciding my fate. I want to assert my right to know. I hope that will be in the AI law: transparency and explainability. I want kids to be able to read the script in terms of the consent form rather than these long spiels of standard form contracts, which are very difficult to read.

The puzzle is the superpower rivalry. The AI setting is also very constrained, so be very careful there. There might be imbalances in data sets and algorithmic biases, along with intellectual properties, copyrights, and patents. Famously, everybody's buying up graphic processing units linked with the new generative AI, which can create, which can write, which can paint. What about super AI that is coming in, and what about when there is no electricity? What do we do? Together with human control versus tech autonomy. What humans are to control: democratic humans, authoritarian humans, or self-control by the robots?

The challenges very quickly include subliminal drive of a destructive kind, social scoring, social profiling, targeted vulnerability selling adverts through adverts to children, for example; also automated attacks, state control, excessive data collection, algorithmic opacity, and robotic screening without informing the data subject. There is also the "Overdo" of content moderation, with data taken down too much by the industry itself through self-regulation, even though there is an oversight board. Millions of items are taken down by the oversight board of the big platforms, sometimes unjustly, sometimes arguably, as well as competition for control of power and chips. There is the interface with broad interpretations of exceptions to data privacy, such as national security, and there is also the clandestine mapping of mental state, known as psychography. This might entail the metaversal - goggles that you might wear which can also record your facial expression and nose twitch, and they can paint what you are in terms of your psychography. They can profile you in an unbalanced manner, which will affect you and your family, ultimately, even though we do not deny the medical and labour-related benefits, and the impact of cumulative data should not be underestimated as contrasted with minute data.

What plagues me is this: what about a world without electricity? In that country where there is a war in Europe at this point in time, one bomb, one disaster from flooding, there is no electricity, and what do we do? The other tech, the human tech of survival, is also very important.

What about future directions? A mix of hard law and soft law maybe, but we have some guidance already, the Sustainable Development Goals (SDGs), and we have the UN Secretary-General's Common Agenda. The agenda of the day is there already to some extent: the need to connect people fairly, avoid internet fragmentation, protect data, apply human rights online and offline, introduce accountability, promote regulation of AI, and digital commons whereby we can share some information free as a public good.

We have a summit of the future in 2024. It is likely that we will head towards a global digital compact. A compact is not a treaty; it is more of a soft law, it is like the SDGs. I do not think they are going to go for hard law; it is too difficult to negotiate internationally; we will wait and see. Will the UN do monitoring of AI and the like? Well, we are also bound, maybe, for a code of conduct, soft kind on information integrity, as well as implied action against misinformation and disinformation, but not forgetting the need for human capacity in terms of an educated and empathetic, sympathetic person in his or her or their relations with others.

Practical options involve many stakeholders: technological education with empathy, overcoming the online gap, making some data digital commons, and peer support such as counter speech to protect those violated by cyberbullying. Balance contractual obligations, your click and the long contracts there, Yes or No, should be legible and understandable. Accessible filter and techno screening based upon human rights also. Enlightened self-regulation may be mixed with co-regulation and regulations at large, as well as due diligence to evaluate, to test what might happen, and to prepare as a precaution with measures to mitigate or lessen the risk. Maybe from a consumer perspective, certification of products, together with labeling and consumer leverage, as well as stakeholder participation in the whole process. Potentially needed also are measurements such as technology index, which we have, or gender index scorecards, and so on, in terms of progress rather than regress. As a person dealing very often with implementation issues, guided by those directions, I would say there is a situation here, very easy in terms of the preferred options and implementation tools to match between good law and enlightened technology.

What do we need? We need good laws. If we have not-so-good laws, try to avoid implementing them. Please suspend them. There are so many not-so-good laws globally. These are the Needs as follows: good policies, good programs, good practices, good mechanisms, good resources, transparent data (disaggregated), good education, good remedies, and good space for changes and reform.

A final reflection, because we are dealing with the law. International law is often a guardrail in regard to state sovereignty - what a state claims as untouchable or nearly untouchable. Traditionally, international law was very much based on respect for some degree of state sovereignty in terms of the state's rights and obligations between states and between states and other actors, in particular, international legal persons like the UN. Later, that notion has become more oriented towards obligations towards people and populations, dealing with the animate, the sentient, the person who feels, the community that feels, individuals, families, and communities.

Today, the stakes are extended more now to the environmental perspective with the entries of life at stake, living beings, the right to nature, the right to breathe, as well as the right of nature to be protected. Humans should be stewards for the next generations but also respect the world as

the world in its cosmology as well as its ecology. Now, we are faced with inanimate non-humans. They do not feel, or at least we do not think they can feel, the non-sentient, such as AI. Perhaps we also need an evolved understanding and transformative understanding of the new sovereignty at stake. It is the advent of a shared human sovereignty that is now at stake, especially when we are dealing with the inanimate and the non-sentient.

We claim, all the time, the need for human control, but we are also faced with power play on this, power control, checks and balances in regard to power. And I believe, maybe just to tease you a bit, there are three Human C's that differentiate us from non-humans that should be part of our understanding of sovereignty, and these are the three C's as a present for you: **Conscience, Consciousness, and Care-Consideration** towards life, that is what makes us human and sovereign in what we are, as well as the state that should be part and partial of us.

If that is the advocacy of a new sovereignty shared between humans in the face of non-humans that are coming towards us, then perhaps there is a final puzzle that we can all unravel together. Demystifying our law and more:

- **Humanising through shared interface,**
- **with material and spiritual embrace,**
- **to be and not to be**
- **and choose to be,**
- **not only techno-savvy**
- **but also tech-yes happy**
- **……**
- **so simply to be free.**

Thank you. We have time for questions.

Q&A

Dr. Anuson Chinvanno

Thank you very much, Professor Vitit, for that very stimulating and also provoking presentation. Now we can take comments and also questions. Who would like to start? Well, if nobody wants to start, I will take the organisers' privilege to ask you the first question.

In our dealing with cybersecurity and cyberbullying, we often talk about the abuse by the authority, abuse of law, abuse of regulations, or abuse of policy. I think you made these points quite clear in your presentation. But what about the abuse by the individual? I think a lot of these cases have led to crime. When we talk about cybercrime, they are usually because of the abuse by the individuals or groups, private groups of people, criminals or whatever. How do we deal with those in terms of international law?

Mr. Nontachat Jintakanond

Thank you very much. I have two questions. First of all, let me tell you where I come from so you understand the questions I have. I come from the National Broadcasting and Telecommunications Commission, and I'm the executive director of international affairs. So, I also work with the International Telecommunication Union.

My first question would be this. The issue that we discuss a lot under the ITU is, with all the technology coming, we have been regulating the telecommunications, but what about the new technologies? And we are even puzzled in that forum as to how to regulate them. We start from OTT (Over-the-top). Now we have AI metaverse. So I would like to hear your view about that in terms of regulations.

Second question, now we are also negotiating many free trade agreements. Before this, the free trade agreements are about trade. Now we start talking about digital trade, and often, we start discussing these too. Do you view it as the opportunity or the risk, and should we, as the negotiators be careful or be cautious about this, about where it's leading us? That would be my two-part question. Thank you very much.

Dr. Siwanuch Soithong

Thank you, my name is Dr. Siwanuch Soitong. I'm from the Mirror Foundation. I'm the head of the Mirror Foundation Legal Clinic. I am very thankful today that you let Thai people understand about technology that's going to affect us a lot. We're taking care of a lot of vulnerable people in Thailand and also outside of Thailand. And what Professor Vitit said about the young generation who are going to be empathetic with each other to create a new population to understand and use AI.

So, I think a lot about how the children of Thailand and of ASEAN are going to understand this issue. Lately, I have been working on cases of about 128 children from Myanmar who come to Thailand and study in Thai schools. But we have a problem. We expect that they would not get

regular immigration, and would be deported. And right now, they're out of the system of education. So I think a lot of bullying happens on the internet to the children and to the teachers, and I don't know what to do right now. I don't know if it's possible to help them and try to make it better like raising some funds to help them get an education in Thailand and become regular immigrants. So it's like it's passed the 'no empathy' in ASEAN as well. I don't know how we are going to change this because if we are not going to change, it's going to happen on the internet, and many kids are going to consume that. Thank you.

Professor (Emeritus) Vitit Muntarbhorn

Thank you very much for those three important inputs.

The first one is about crime, particularly cybercrimes. We are totally conscious of the need for effective laws, policies, and practices against cybercrimes, and the tools are already there to some extent: general criminal law, cybercrime-related laws, computer crimes-related legislation, etc. Quite a lot of them. The advocacy here is to balance these laws well with considerations of checks and balances in terms of protection for people. The danger or the difficulty is too much discretion for the authorities or with the authorities. International advocacy advises that discretion should be very constrained rather than very broad discretion by the authorities to tak action against people. That is why internationally, in terms of international law and human rights, we have this three-part test. Legality, which is claiming that the law or the action must not be arbitrary. It must be a good law, a transparent rule of law type. Secondly, the dangers and the actions relating to dangers must be considered from the perspective of necessity and proportionality. The third one is legitimate aims. Part of the problem of many Thai laws in the criminal area is that they do not quite fulfil the three-part test. That critique is not because of me necessarily but because of the UN monitoring as a whole, which suggests that we need to reconfigure some of our laws, including our Emergency Decree, which is very famous on many fronts, computer crimes law and various other, and crime-related provisions of the criminal code.

It is not a negation; it is not a denial of the need for laws, but to have more balanced laws with checks and balances. If you work towards the international setting, I have already added the caution that we now have a process of drafting of a cybercrimes treaty subject to power play. At this point in time, one should be very cautious because there are provisions in the draft which are very extensive and beyond the limits of what we would advocate internationally, including the potential of very free data flows between law enforcers without due regard for privacy, various basic freedoms, presumption of innocence, and so on, that can be affected by overzealous exchange of data. So, that is the advocacy, and that is why I said if you really want to look at an example, not because I am advocating Europe, but it is just that some Asian countries are also parties to the Convention, the Budapest Convention is generally regarded as the more balanced convention of something very specific in terms of attacking cyber-related crimes. This implies particular listing of crimes such as child pornography, fraud, etc.

A lot of this is going to be linked with some of the UN-related agencies, the multilateral agencies such as ITU, in terms of communications as well as copyright, together with the human rights arm of the UN. We have a sort of direction already with regard to the UN's Common Agenda that I was voicing, as well as the discussions towards the summit of the future next year. I am sure that ITU will be very much involved there. The messaging in terms of international negotiations is that it is highly likely that many of these considerations will creep into the negotiations of free trade in the future. So, the invitation is really to take stock of the various options that are now arising.

There is the European link. Not because we like Europe or not, but European laws, not human rights laws necessarily - they are economic-related laws - which are catalytic. This is from the European Union, 27 countries, not from the Council of Europe, 46 countries, with one big country now expelled. We're not talking about the Council of Europe; we're talking about the impact of the European Union, the slightly extraterritorial impact actually, with now the Digital Services Act applying together with sanctions for Thai companies also working in regard to Europe.

In 2024, we will have the Digital Markets Act, which will impact more on the competition between different types of companies together with the digital spectrum, impacting Thailand as well. So that is the European nexus, so to speak. We are negotiating a free trade area maybe with Europe now, so it comes in. My advice is to be slightly prepared, and we do not need to reject it because we're also evolving an AI law at this point in time. I said already the AI law is already influenced by Europe, but there are some elements that I want to have as clear elements, such as I want the right to know that there's a robot there, and I want it explained. And that is part of the UNESCO framework internationally of explainability and transparency, as well as some of the legislation arising in the US. That is a caution; it's coming, like it or not.

We are not necessarily in favour of that region or whatever, but this connectivity, particularly of the cyber as well as the cyber laws and various trade-related areas, is coming in, and ASEAN itself is interplaying with this. But, as I said, the ASEAN framework is much more a facilitative framework. We want to be in the lead rather than one that focuses very much on basic protection, such as protection against too much targeting of adverts to various vulnerable groups, such as children.

Or now we just had a court case in Europe just a couple of months ago, the potential merger of data from different platforms owned by one mega, and Europe just said you can't do it without consent of the European Commission/Court. There are these safeguards, but that's the hard law approach, whereas in the United States, you have a mix, you have state legislation separate from federal, which can go either way. I mean, you have got California at the moment with a draft law on transparency as well as the prohibition of targeting of AI in regard to children or various vulnerabilities. Or there is another law in another state which wants to set up a supervisory body or to be supportive of the federal government. So, different ways of approaching harder and soft without necessarily a federal approach yet, subject to the discussion between the top gentlemen of

the executive branch with the mega companies the other day, which invited a soft law commitment from the big platforms in the United States. So, the US is a conglomeration of different approaches.

What I am saying now in regard to what you have to deal with is that it is part of the trade and commerce process very much, together with the enhancement of the rules next year in regard to a forthcoming Digital Markets Act, which would be even more circumscribing in terms of basic protections and the famous word - the guard rails. Finally, children and others. Well, in fact, already we have flagged the concerns of children for a long time, particularly against abuses on the internet. And there are already many laws here and there.

There is a Child Online Law in the US Various Thai laws can also be used. We have the Child Protection Law, and we have the criminal code, which has been expanded to cover child pornography on the internet. Computer crime law can also be used to protect children in Thailand, thus there are quite a lot of laws. But the whole spectrum invites different stakeholders to come into play. What about the business sector? It's not adequate just to have a state law. We want business sector commitment, additional maybe self-regulation and monitoring against abuses on the internet. Or maybe to work with the children themselves in terms of the child support system's different entry points. When a child is attacked on the internet, often, what is the person? What's the kid to do? The person wants some psychological support, obviously, to deal with it. So, peer grouping up, call it peer counseling, is also possible.

And the other side of the fence is this: we, parents, also have to learn to enable children not to be too dependent on memes and on computers all day and all night. It is just not logical or human. There must be some special times to liaise with technology and to stop at a given time to let the ordinary elements of being human operate: leisure, talk, breathing, and writing, rather than being fixated on the digital.

Today, the other danger is this: previously, we always said that technology was value-neutral; it's the humans who manipulate technology. But today, the world community is coming to the conclusion that technology is no longer value-neutral, especially if it's self-automated together with synthetic data that's coming into play. It can also establish its own values increasingly and take up values which might be detrimental or beneficial to humanity. But the whole point is that we don't want that to happen because we feel and we still claim that humans must be in control and must be in the loop. We still claim it. To operationalise it is not easy, precisely because there are power relations behind it: control, rivalry, as well as democracy versus non-democracy, particularly at play in Asia, which is the most populous continent on earth.

Please look at a package of strategies and not forgetting the human interaction elements, the humanisation process that goes beyond just a law or technology. Parents also have a role in this; other kids have a role in this; school teachers have a role in this. The empathy factor of socialisation is very important. You know, I am a teacher by coincidence, and for two to three years, I was online. And I give you one example. I would have to switch my face on all the time; that's facial recognition, but the students, sometimes none of them switched on the screen, and they never gave a thought to it. I, as a very relaxed teacher, had to question myself as to what psychological strategy I would get into.

So, I consulted many friends, and some said, "Oh, order", but I do not mind students sleeping in my classroom as long as they do homework. Alright. But what do I do with these 20 blank screen potholes, all dark or more? So, after consultation, a very humanising approach of socialisation, through which I learned, I said to the students, I always say, *Nong Nong*, brothers, sisters, would you like to try to switch on, unless you have a reason not to switch on? There, I think, was a really nice human interaction. Not because of me, but because of the wisdom of others, they started to switch on, and one or two said, "I'm not switching on because I am borrowing the computer and I am in a place which is not very nice", which is a fine reason for me – the teacher - to accept the blank screen. So, okay. And finally, you know, the switch on revealed one nice student who had this background of Versailles behind him, whereas my background was my bedroom, a very unruly bedroom in terms of not very orderly bedroom! It was the privacy being revealed. The psychology of online privacy should be studied!

So, in the end, yes, they switched on, and then they came back to university after two to three years, you know, students from year one and from year four didn't know each other, a lot of them, until I invited them to dinner. And, you know what they called themselves? I was just shocked, as a *hubot.* They said "Khun" to each other, young people saying "Khun" to each other. The "Khun" in Thai is such a distant thing, you know, particularly between the young. I was shocked they were not calling each other by nicknames. So, through dinner, lunch, talk, and chitchat, they started to ease towards each other. These are human elements that should not be forgotten in terms of our socialisation process. It is not just technologisation; it is humanisation through shared education and social socialisation that we also have to personify. Thank you. Any others?

Dr. Suphanvasa Chotikajan Tang

Sawasdee Ka, Ajarn. Suphanvasa, Director-General of the Department of Treaties and Legal Affairs. Thank you very much for your enlightening presentation. It's always a pleasure to actually listen in, and I'm sure you had great fun preparing this presentation. You gave me a lot of food for thought, and the one thing that struck me is actually, whether we know what we want yet from the law that we're trying to create here.

Regarding the puzzles that you put on the screen, I really don't have an answer yet on what the direction is as the legal advisor for the Thai government on international law. I'm still looking for that point where the government, what is the role in terms of creating that international law that we want to see. I think technological advancements have always been the benchmark of human advancement, of human well-being—how well we've been doing. And really, technological advancements are the test of how much power you have in terms of political engagement. Those who have the power are those who have the say in how the politics, and how the relationships are defined.

So, I think there are two sides of the coin. There is the good side of technology and, of course, the bad side of technology. Regarding, FTAs that we're negotiating with the EU, of course, we would like to see that digital commerce happening with the EU. But, of course, it comes with

a price. We also have to have our own kind of standard to be able to guarantee to the EU that they're convinced that we have the right background to be able to engage with the EU. But also, the fact that the government is keener on doing regulation—keen to a point where sometimes we go overboard, like the issue you said about the cybercrime convention that's being negotiated right now. We may go overboard in trying to secure that confidence government officials need. But in terms of facilitation, which I think is something that international law really needs right now, we're not really sure of how to go about it. Because for technology, it's not the government that drives it; it's the private sector. And the government cannot do that without the private sector because we don't have the funding needed.

So, how do we become the facilitator? How can we make international law in order to have the technological advancements that are needed? Thank you.

Dr. Saliltorn Thongmeensuk

Thank you very much, Professor. I'm Sililtorn Thongmesuk from the Thailand Development Research Institute, and I was also a legal expert in the AI Governance Clinic of ETDA. I do have a few questions, but actually, it's very similar to those asked by the person before me.

First of all, given the influence of the EU GDPR on the domestic law of many jurisdictions across the globe, will the EU AI Act have a similar influence on the domestic laws of many regions across the globe? And secondly, you did mention the different levels of regulations of AI: soft law, hard law, and also ethical guidelines. Do you think the implementation of hard law in Thailand would kill the industry, or is it necessary from your point of view? Thank you very much.

Mr. Printorn Kordumrong

My name is Printorn Kordumrong. I'm from the Thailand Institute of Justice. I would like to thank you very much for such a great and innovative talk today.

My question for you is this: Is international law able to keep up with the development of emerging technologies? And if not, what do you think are some of the gaps in these checks and balances that you have identified? Is it primarily an enforcement issue that you think is the problem?

The reason why I asked is that, in all of our experiences, I think that the drafting and amending of legislation is usually a game of catch- up with developments in society and particularly with these technologies that are now sort of crossing into the realm of science fiction, seemingly at this point. I'm just wondering since there's the principle of no punishment without law, I'm wondering if these gaps can prevent people's justice needs from being met. So, that's my question. Thank you.

Professor (Emeritus) Vitit Muntarbhorn

Thank you for all excellent comments and questions. Number one is the role of international law, particularly in dealing with new technology. International law and human rights, these international elements are basic minimum, not maximum. States should not do under the

minimum, if states and other actors wish to do more, great, but don't go under the minimum criteria of preferred operations and respect for humanity. I would start there. What we're talking about is not a negation; it doesn't deny initiatives of countries and regions to go beyond the basic minimum in terms of basic protections of humanity and nature. And I would say that lawyers should also be very open to an understanding of power play in terms of what's behind new laws, new conventions, and so on, as I highlighted through a certain skepticism towards the new cybercrimes law.

So, who has the democratic hand behind all this? In Asia, we have to be very careful because, on many fronts, we have constrained civic and political space in regard to guidance of preferred development of international law. I've already listed various possibilities in terms of the puzzles and also the guidance from UNESCO and very easy tests. Is it safe? Is it secure? Does it respect privacy? All those are elements which can help us in terms of testing and due diligence, meaning we need to take stock of dangers that might arise in terms of impacting humans and nature. Take precautions. Do no harm and build those mitigation elements into our risk assessment and risk-related measures.

So, in that perspective, the lawyer doesn't/cannot provide all the answers at all. In fact, part of the problem of negotiations of some of these treaties internationally is that those sitting there tend to come from lawyers and some ministries but not engineers, not ethicists, not stakeholders, civil society, or human rights defenders. These are little loopholes that we should fill in in terms of the shared negotiation process if we're working towards hard law. Of course, if it is soft law or hard-soft, we know today that the role of industry is very, very important. And the question also is, which industry? Because we know very well that in terms of self-regulation, the most famous ones interrelate with the mega companies that are all over there, not the mini ones over here. This means that the power relation in terms of enabling developing countries and developing communities to evolve a certain technology is also very important.

We're back to the other principle that I listed in terms of puzzle: equity, the sharing of resources and power in terms of also, technological resources, education, and financial plus non-financial resources. That is why you have this dynamic always now increasing, basically in terms of if you can negotiate multilaterally, what cake do you provide for the developing countries? But I would see it not as a sort of give-give in terms of a donor and donee but more as a sort of shared responsibility in terms of sharing in terms of equity of resourcing, some of which were built through unbalanced power relations, including colonization in the past, which also made use of technology. You know, your Industrial Revolution. Where did the coal come from, or where did the iron come from if not developing countries? You see, so you have that historical perspective which is very important, also enhanced by the need to teach histories so that we can understand the power relations from the past that still shape the present.

That is calling for a more rounded approach in terms of negotiations together with the multiplicity of stakeholders and actors in the negotiation process rather than just enabling you or me to go and sit there and negotiate. A lot of the wealth of wisdom coming to me through here is through many other sources, not because of the law at all, but through readings and chit-chats with many others of different disciplines in an interdisciplinary, intersectional world.

Secondly, the influence of Europe's General Data Protection Regulation (GDPR) and the forthcoming AI law. The draft AI European Union law already has influence in terms of the Thai draft decree or regulation on AI. As I said, the prohibited AI in the draft AI law of Europe is already there in the draft Thai law—no social scoring, remote surveillance, facial biometric probably there, and as well as social scoring.

So, we are already influenced by the undercurrents or overcurrents in Europe. Why? Because it is the most hard law-oriented approach at this point in time, with their safeguards, which have been through a very consultative process. The European law that comes through, not because I am a lawyer trained in Europe, but it goes through a very participative process; initiation from maybe the European commission plus, and a lot of vetting through the European Parliament, which was open to parliamentarians but also their colleagues from other industries. And then now towards the political arm, which is to the Council of the European Union, so it goes through a very filtered process of coming through as legislation and impliedly it has extraterritorial implication. So, actually, the moment you know the matching, particularly in preparation for FTA and the like, is that you have a conglomeration of laws arising in terms of digitalization ranging from the General Data Protection Regulation to the Digital Services Act, which increases scrutiny and sanctions, to the AI law coming up as well as the Digital Markets Act coming up next year and whatever else. As a very integrated regional system of a supranational kind, which has impliedly extraterritorial implications.

So, it's there. We're not saying it's the best necessarily, but take stock of it and build on it. And you might have certain flavors locally that you could add to it. The approach of many Asian countries is to have very strong exceptions. That's what you should be very careful with—the right to privacy maybe or safeguards, but strong exceptions on the basis of national security. Even now, the little legislation, subordinate legislation coming through in Thailand, is about exceptions. If you look at it, some sectors are exempted from the Personal Data Protection Law—security, banking, etc. So be careful because even if there's a sort of slightly enlightened framework within the political setting of a certain society, often constraints creep in because of the power base justified by various rubrics such as national security, public order, public health, and public morality, and that's why international law is very careful about those rubrics and tests them through various strong criteria, such as you, the authorities must prove legality, necessity/proportionality, as well as legitimacy.

Finally, from a friend in terms of the Institute concerned that I know very well, the way that it is emerging is that it's not an either-or situation. You might have hard law, but it's happening more at the regional level, but the regional doesn't necessarily end there. You have the multilateral, and what we've been talking about is that if you look at the multilateral, it's actually quite difficult to have hard law. Why? Because there is power play, and even for the CCW, the Conventional Weapons Convention, most Asian countries are not parties, even though I would say it's not a bad convention. I mean, we should forbid blinding laser weapons; we should try to clear explosive remnants of war and be helpful to developing countries, but we're still not parties, many of us. And we're not there to expand that CCW, and now the interface is that there's a new treaty arising,

maybe through the UN General Assembly through power play of superpowers, which is separate from that older treaty, which is there already to be used. So, we don't need to reinvent the wheel necessarily but to make good use of what we have if we have the political will to do so.

Lastly, on that, as I said, we are working towards a digital compact next year, and I would hazard to guess that it would be a soft law, but it will have many elements there, as listed already, together with the equity element of sharing more. But also, it's there already. I mean, in the components that I listed for you in terms of some regulations on AI. Now, which level? When we now see the regional level, we now see the national level, but the international level is going to be difficult because of power play, which is part of life, but we have to be very careful. And if they're going to come out with a very broad draft such as the cybercrimes law, then we have to be doubly careful, not because we're lauding a particular region but because we have lessons learned in terms of shared wisdom from different regions, We should not forget, as I said, the simpler elements of humanisation, socialisation from which we can learn from very simple communities like the best teachers, the best parents, the best young people, already helped in terms of helping as peers or as communities, providing a certain cushion and embrace for those kids and others who might be impacted upon negatively at this point in time and in the future.

Mr. Juthakeart Montapaneewat

First of all, thank you, Professor Vitit, for this thought-provoking presentation. My name is Chutakiat Mantapaneewat, and I am counsellor from the International Security Unit, Ministry of Foreign Affairs. I wish to thank the International Study Center for organizing this wonderful event as well.

I have a specific question regarding cybersecurity in terms of peace, international peace and security. I'm part of the UN negotiation process on cybersecurity, and the discussion that has been going on for quite some time is the applicability of international law in terms of cybersecurity. For the past few years, we've seen the use of cyber in armed conflict, and I think cyber warfare is inevitable in the future. Of course, we have the IHL, but my question is, of course, as Professor Vitit mentioned, that power play is really important in terms of negotiation for the new treaty. The new treaty on cyber security is one thing that we have been considering for quite some time. I think power play will be a really important factor, but for the IHL, as you and everyone may know, the cyber domain is totally different from the physical aspect of armed conflict. So, do you think the existing IHL is enough to cover the use of cyber tools for armed conflict or civil warfare in the future? And because the principle of distinction and proportionality may be different in terms of physical warfare compared to cyber warfare. First of all, do you think the existing IHL is enough? And secondly, if not, what is the way forward in terms of legal or academic aspects? Do you see we will have the new additional protocol to the Geneva Convention, or do you think a totally different convention or treaty should be the way forward for us? Thank you.

A Participant

I have two questions. The first question is, do you see the possibility of a law against discrimination for AI? Because, as people, we are prohibited from committing a hate crime against another based on gender, nationality or ethnicity. But when it comes to AI, I think AI has this feature where it can recognise faces and or certain characteristics, and it may deem that person, for example, a terrorist. I may go for an extreme case. There are some occasions where the AI computes certain characteristics of people, deems that person a terrorist and then kills that person. Do you think, there will be a law against discrimination in this respect or do you think there will be a development for human rights law?

My second question. I think you have already given the answer to the question, but you have mentioned that when the state wants to intrude on people's privacy, it has to prove the necessity of that act. But my question is, if the intruder of privacy is the private enterprise and that private enterprise is far more globalised, that is power transcended beyond the border of the state. How do we prevent the invasion of privacy? Based on my understanding, I think at the time, we depend mostly on the domestic law of the host. Do you think there will be international law to cope with that? And do you think that this challenges the concept of sovereign state? Thank you.

Professor (Emeritus) Vitit Muntarbhorn

Thank you very much. Really good questions. To what extent does existing law on warfare, international humanitarian law, the law on the conduct of hostilities, as well as protection of victims apply, to cyber issues? The answer is that it's not clear. Some elements are clear, but not all elements. As you heard already, the expert group dealing with autonomous weapons already said that basic principles of humanitarian law apply, meaning, for example, the principle of distinction. You must distinguish between military and civilian targets, the principle of proportionality, and military necessity in terms of ensuring that military advantage is a consideration, but it must not exceed in terms of proportionality the harm done to the objects or perhaps collateral damage for civilians.

Now, if those are basic principles which are there already, the complications in regard to warfare, particularly in regard to the international law on this in terms of the shift from an ordinary situation to a warfare-related situation 1) in legal terms, the law concerning the lead-up to armed conflict (jus ad bellum) and 2) the law applying during armed conflict (jus in bello). The complications include: number one, the notion of attack is usually one that's a physical notion of an armed attack, but what is and what about a digital attack? There's a bit of a query at this point in time, and we are differentiating between a kinetic relationship and a non-kinetic relationship. Kinetic means a computer or cyber, system or cyber-related attack, but it's a physical one of a bomb accompanied by the code, the cyber attacking someone. And that is differentiated from a general cyber digital attack, which might be in a very grey area of when it happens and where, and in terms of accountability. The nearest we have in terms of discussion on this is under soft law discussions of a slightly technical academic kind, but still important in terms of prevention and precaution, and that is known as the Tallinn rules of the Tallinn Manual, Tallinn being in Eastern Europe.

The experts under that initiative came together to evolve a certain understanding of this, but as I said, it's still in a state of flux. But we can still try to apply those basic principles such as distinction, proportionality, and necessity, even though the attack factor might not be clear. The other is the objective. Usually, when we are dealing with laws of war, we are dealing with military objects or civilians or civilian objects, something very tangible. But what if it's an attack on something not tangible in terms of the digital system? The machine is still there, but it doesn't function anymore. So does one use materiality as a test for the application of the law on this front when the machine is okay but the data system is totally wonky?

There's a debate, and maybe from my perspective, maybe we should also think about the harm done because the harm done might be that that computer system if it's dysfunctional or nonfunctional, might be harming a lot of people. Why? Because it might not be able to protect people. So you're back to square one in terms of law and policy and the taxonomy of relationships. What is the causation and causality in terms of relationship? I would say that we shouldn't forget the consequences that arise in terms of the attack even though the computer might be there, but if the system is dysfunctional and has an impact on lives around the computer system, maybe it's one that should give rise to accountability. So that's the debate at this point in time.

Also, I think they're very simple precepts in terms of the strategy to prevent, the strategy to protect, the strategy to provide remedies and the strategy to enable people to participate. Those are very simple strategies which enable us to evolve a certain protection system in terms of the laws that we wish to see, whether in terms of cyber or other elements. Lastly, on AI law and, I think, the issue of speech and hate speech and agency and the like. We do have standards. The international law on this is actually drawn from a human rights treaty known as the International Covenant on Civil and Political Rights, and freedom of expression in regard to 'I like you, I dislike you' is shaped by Article 19 and Article 20. Article 19 ensures your freedom of expression, my freedom of expression globally, and Thailand is a party to this, subject to two exceptions: one is defamation when you or I say nasty things about other people, and secondly, when it's in breach of public order or public health or national security. But having said that, all those exceptions are still subject to the three-part test I was referring to earlier in terms of the government still needing to prove legality, necessity/proportionality, and legitimacy. Now, that's the general framework for freedom of speech, which is not an absolute right.

The other one, which is additional, is in regard to hate. International law doesn't prohibit hate in general unless it falls into this notion of incitement to hatred, which falls under Article 20 of the Covenant on Civil and Political Rights. In other words, it's the relationship of 'I provoke you to do something nasty to third parties,' a triangular relationship, rather than my hating someone as a bilateral relationship. And that is where the law is needed, according to Article 20 of the Covenant on Civil Rights. So that's the framework in terms of the rather old law, but today, because hate speech also evolves and is linked with information disinformation, you need other strategies. That is why I think the Z Generation is going to move towards an information Integrity-related Code of Conduct, and soft law next year to invite strategies, multiple strategies to tone

down the hate in this bilateral relationship, whereas the trilateral relationship of 'I provoke you to hate and do something nasty to see' is already covered by a prohibition of Article 20.

The bilateral relationship depends upon lots of things. It depends upon education so that I can be empathetic to you, good socialization, maybe internet industry help. We have the Internet industry; all these contracts that you click on have community standards that are sometimes higher than international law or national law. Homophobia is forbidden on the internet; I mean, you can't attack gays; you'll be taken down. But that's not the law in many countries; that is a higher standard than international law, actually, in the traditional sense. So the internet industry can also take charge of setting a high standard in this self-regulation subject to monitoring by the oversight board that they have, and the oversight board of one big one mega-platform takes down millions per year of hate-related type speech, including politically related hate speech, which is prominent in some countries, including some democratic countries too.

But that's one of the options also; it's not the only option. We have a techno option. Filters also. And we have the other option. I used to help the UN on LGBTI; I got a lot of hate speech, and my successor got even more. What did I do? They were not hate speech to the extent of defamation, and I didn't want to get involved in national security either; it was my feelings, and how would I respond? How do you think I responded? I used to sit down and pray for people to be kinder to other people; that's how I responded. So please don't think that law or technology is going to solve everything; there is a non-material element of how we deal with not-so-nice things, which can be, dare I say it, somewhat spiritual and not necessarily religious either. And I still pray for not-so-nice people to be nice; I make merit, I give money, not to—I don't like to give money to temples very much, but I make merit and pray that autocrats will be kinder to others because I have to deal with them here and there.

There are different ways, so please don't just look at one strategy. But there is much more than one, and it's both material, non-material, tangential, non-tangential, human, personal, physical, and non-physical spiritual. So, with that in mind, explore our options, and. We can start at home, enable our kids to have good sharing time with us and talkative time rather than be fixated on digital, which I don't reject, but I don't think we should have digital, the mobile on the dining table all the time when we should be chit chatting nicely or even, even if we were not nice, we try to chit chat nicely to empathise a bit more.

So, with that in mind, I would like to thank the Institute very warmly, my friend Dr Anuson, and friends and family on the internet and others. I have one final question for you: in three billion years' time, when Andromeda meets the Milky Way, whatever you call it, "Andromeda", "Milkomeda", what will be your thought at that point in time when it meets? What will be the words on your lips as part of humanity when Techno meets Cosmo in the cosmology of things from here to the other eternity? What will you say to yourself? Can you say it to your neighbour? We should collect this, and please send it to the Institute. I am fascinated.

Do you know what I will say? Do you want to hear? Yes, you, my friend, incitement; you want to hear? I will say this. I will say:

“Empathy, Friendship, and Love transcend all.”

Thank you.

Dr. Anuson Chinvanno

Thank you very much, Professor Vitit, for that last word. I would say that I will not be here in three billion years. Thank you very much, everybody, for attending this event and making it very lively. I hope you get some provoking ideas to go back and think about. This is something that will affect probably many people here of the younger generation. I thought this is a good opportunity for you to get some food for thought. So ‘bon appetit’ and let's hope we will see you again at our future events Thank you very much.

Annex 1

Biography of Keynote Speaker

Vitit Muntarbhorn is a Professor Emeritus at the Faculty of Law, Chulalongkorn University, Bangkok. He is a graduate of Oxford University (M.A., B.C.L. (Oxon.)) and Universite Libre de Bruxelles (Licence Speciale en Droit Europeen (Brux.)). He is a Barrister at Law (The Middle Temple, London). He teaches International Law, Human Rights and related subjects.

He has held a number of *pro bono* UN positions, in particular the following: the first UN Special Rapporteur on the Sale of Children, Child Prostitution and Child Pornography; the first UN Special Rapporteur on the Situation of Human Rights in the Democratic People's Republic of Korea; the first UN Independent Expert on Protection against Violence and Discrimination based on Sexual Orientation and Gender Identity. He was the Chairperson of the UN appointed Commission of Inquiry on the Ivory Coast (2011) and a member of the UN appointed Commission of Inquiry on the Syrian Arab Republic (2012-6). He also served on the Advisory Board of the UN Voluntary Fund for Technical Cooperation on Human Rights (Geneva) and on the Advisory Board of the UN Human Security Fund (New York). He was a UN University Fellow at the Refugee Studies Programme of Oxford University. He was, for a decade, a member of the International Labour Organization (ILO)'s Committee of Experts on the Application of Conventions and Recommendations.

He has been a consultant to many UN organisations and programmes, including UNESCO, UNDP, OHCHR, UNICEF, UNHCR and ILO. Currently, he is UN Special Rapporteur on the Situation of Human Rights in Cambodia, under the UN Human Rights Council, Geneva (2021-). He has taught in several countries, including the UK, Canada, Japan, Republic of Korea and France. He is a member of the Advisory Board of the International Institute of Human Rights, Strasbourg. He served as the Alternate Thai member on the ASEAN High Level Panel that drafted the Terms of Reference to establish the ASEAN Inter-governmental Commission on Human Rights. He was, for several years, Co-Chairperson of the (civil society) Working Group for an ASEAN Human Rights Mechanism. He helps non-governmental organisations in Thailand in a *pro bono* capacity.

He has published widely on International Law and Human Rights, and he is a columnist of the Bangkok Post newspaper. He has written over 20 reports on a variety of issues for the UN. His books include *The Status of Refugees in Asia* (Clarendon/Oxford University Press); *Unity in Connectivity: Evolving Human Rights Mechanisms in the ASEAN Region* (Brill/Nijhoff); *The Core Human Rights Treaties and Thailand* (Brill/Nijhoff). His latest book is *Challenges of International Law in the Asian Region* (Springer).

He has won a number of awards nationally and internationally. He is the recipient of the 2004 UNESCO Human Rights Education Prize. He was bestowed a Knighthood (KBE) for his international work on Human Rights in 2018.

Annex 2

SPECIAL LECTURE ON

INTERNATIONAL LAW AND EMERGING TECHNOLOGIES

SEPT 5, 2023
13:00-15:00 HRS.

By Professor Emeritus **Vitit Muntarbhorn**

Faculty of Law, Chulalongkorn University;
UN Human Rights Special Rapporteur

NARATHIP AUDITORIUM
MINISTRY OF FOREIGN AFFAIRS
SI AYUTTHAYA RD.

Photos of the Event

The International Studies Center (ISC) aims to encourage the studies and analyses of relevant policies and issues in various aspects of diplomacy and international affairs, including foreign policy, international economics, international law, and international and regional organizations, as well as to create opportunities for policy and issue related discussion for the benefit of the formulation and conduct of diplomacy and foreign policy, while promoting public awareness and understanding of major foreign policy issues, through such activities as lectures, seminars, experts discussion, publications and broadcast.

Seminar Report is a series in ISC's publications which records proceeding from seminars, discussions and book launches organized by the International Studies Center.

ISC Seminar Report Series

Seminar Report
Book Launch and Discussion | Rivers of Iron: Railroads and Chinese Power in Southeast Asia
by David M. Lampton, Selina Ho and Cheng-Chwee Kuik (Authors)
ISBN 978-616-341-109-9

INTERNATIONAL STUDIES CENTER (ISC)
The Government Complex (Building B, 8th Floor),
Chaengwatthana Road, Bangkok 10210, Thailand

email: isc@mfa.go.th
website: www.isc.mfa.go.th