យោបល់លើសេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន

Comments on the Draft Law on Cybercrime

ស្ថាប័ន៖ Name of Entity:	ក្រុមការងារសិទ្ធិឌីជីថល Digital Rights Working Group
ឈ្មោះ៖ Name:	
តួនាទី៖ Position:	
លេខទូរសព្ទ និងអ៊ីម៉ែល៖ Mobile and Email:	
កាលបរិច្ឆេទនៃការផ្តល់យោបល់៖ Date of Submission:	
ឯកសារយោង៖ Reference:	

អត្ថបទដើម **Original Text**	យោបល់ និងហេតុផល **Comments and Reasons**	សំណើកែលំអ **Proposal for Improvement**
Article 1: Purpose This law aims to ensure the integrity of the use and management of computer systems and computer data, protect security and public order, and protect the rights of individuals by setting out measures to deter, prevent, and suppress cybercrime.	Lack of specificity and clarity of the phrase "protect security and public order"	This law aims to ensure the integrity of the use and management of computer systems and computer data, protect the security of information technology systems and infrastructure, and protect the rights of individuals by setting out measures to deter, prevent, and suppress cybercrime.

អត្ថបទដើម **Original Text**	យោបល់ និងហេតុផល **Comments and Reasons**	សំណើកែលំអ **Proposal for Improvement**
Article 2: Scope This law applies to any cybercrime committed within or outside the territory of the Kingdom of Cambodia which infringes the security, public order, or interests of the Kingdom of Cambodia.	Challenges involved with extraterritorial jurisdiction. Difficulty of enforcement given definitions and articles inconsistent with international law. Lack of clarity regarding international law enforcement coordination procedures and extradition treaties	Add terms "security," "public order," and "interests of the Kingdom of Cambodia" to the definitions in Article 3. Revise article to focus solely on domestic jurisdiction, thereby eliminating any complexities that involve extending the reach of the Draft Law reach beyond Cambodian national boundaries.
Article 3: Definition 2. Intellectual property rights refer to tangible and intangible work and achievement born from the idea of a natural person or legal entity.	Definition should adhere to multinational standards used by the World Intellectual Property Organization (WIPO) in order to improve clarity and compliance. In 1995, Cambodia gained accession to the Convention Establishing the World Intellectual Property Organization. Reference should be made to Cambodia's existing intellectual property laws such as the Law on the Patents, Utility Model Certificates and Industrial Designs and the Law on Copyright and Related Rights. Reference the definition on the WIPO website.	Intellectual property (IP) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce.
Article 3: Definition 4. Unauthorized access means having no legal right, excuse or justification to access the whole or any part of a computer system.	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. Most commonly referred to as "illegal access[.]" Reference the definition in the draft UN cybercrime treaty.	Article 7. Illegal access 1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law, when committed intentionally, the access to the whole or any part of an information and communications technology system without right. 2. A State Party may require that the offence be committed by infringing security measures, with the intent of obtaining electronic data or other dishonest or criminal intent or in relation to an information and communications technology

អត្ថបទដើម **Original Text**	យោបល់ និងហេតុផល **Comments and Reasons**	សំណើកែលំអ **Proposal for Improvement**
		system that is connected to another information and communications technology system.
Article 3: Definition 5. Content refers to general concepts or meanings of communication, including websites, texts, images, graphics, animation, symbols, audio, or video in digital or electronic form, which is information unrelated to traffic data.	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. Most commonly referred to as "content data[.]" Reference the definition in the draft UN cybercrime treaty.	"Content data" shall mean any electronic data, other than subscriber information or traffic data, relating to the substance of the data transferred by an information and communications technology system, including, but not limited to, images, text messages, voice messages, audio recordings and video recordings
Article 3: Definition 6. Computer data means any representations of facts, information or concepts in a form that a computer system can process. This category includes texts, images, graphics, animation, symbols, audio, and video in digital or electronic form and any computer program that can cause a computer system to perform a function.	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. The phrase was removed from most recent draft of UN cybercrime treaty.	"computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function
Article 3: Definition 7. Traffic data means any data related to communication using a computer system and generated by a computer system that forms a part of the chain of communication, indicating the communication's origin, destination, route, time,	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. Reference the definition in the draft UN cybercrime treaty.	"Traffic data" shall mean any electronic data relating to a communication by means of an information and communications technology system, generated by an information and communications technology system that formed a part in the chain of communication, indicating the communication's origin, destination, route,

អត្ថបទដើម **Original Text**	យោបល់ និងហេតុផល **Comments and Reasons**	សំណើកែលំអ **Proposal for Improvement**
date, size, volume and duration, or the type of service used for communication.		time, date, size, duration or type of underlying service
Article 3: Definition 8. Computer system means an electronic device or a group of interconnected devices or related devices that perform automated data processing, including all types of devices capable of data processing, but not limited to desktop computers, laptop computers, and telephones.	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. Reference the definition in The Council of Europe Budapest Convention on Cybercrime.	"computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data
Article 3: Definition 11. Computer data storage medium refers to any equipment or technology that can store computer data.	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. Reference the definition in The Commonwealth Model Law on Computer and Computer Related Crime.	"computer data storage medium" means any article or material (for example, a disk) from which information is capable of being reproduced, with or without the aid of any other article or device
Article 3: Definition 12. Subscriber Information means any information contained in any form which establishes the subscriber's identity, such as name, address, records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. Reference the definition in the draft UN cybercrime treaty.	"Subscriber information" shall mean any information that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: (i) The type of communications service used, the technical provisions related thereto and the period of service; (ii) The subscriber's identity, postal or geographical address, telephone or other access number, billing or payment information,

អត្ថបទដើម **Original Text**	យោបល់ និងហេតុផល **Comments and Reasons**	សំណើកែលំអ **Proposal for Improvement**
network address (including internet protocol address), and means and source of payment for such service (including any credit card or bank account number).		available on the basis of the service agreement or arrangement; (iii) Any other information on the site of the installation of communications equipment, available on the basis of the service agreement or arrangement;
Article 3: Definition 13. Seize means removing and retaining electronic devices or computer programs, making and retaining a copy of computer data directly on the premises, restricting access to the computer system or removing computer data in the accessed computer system, or taking a printout of the computer data output.	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. Reference the definition in The Commonwealth Model Law on Computer and Computer Related Crime.	Seize includes: (a) make and retain a copy of computer data, including by using on-site equipment; (b) render inaccessible, or remove, computer data in the accessed computer system; and (c) take a printout of output of computer data.
Article 3: Definition 15. Service provider means: − Any physical person or legal entity offering the users of its services the possibility to communicate using a computer system or telecommunication system. − Any other physical person or legal entity processing or storing computer data for the persons or entities mentioned in the above paragraph or for the users of	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. Reference the definition in the draft UN cybercrime treaty.	"Service provider" shall mean: (i) Any public or private entity that provides to users of its service the ability to communicate by means of an information and communications technology system; and (ii) Any other entity that processes or stores electronic data on behalf of such a communications service or users of such a service

អត្ថបទដើម **Original Text**	យោបល់ និងហេតុផល **Comments and Reasons**	សំណើកែលំអ **Proposal for Improvement**
services offered by these persons or entities.		
Article 3: Definition 16. Pornography refers to any image that is transmitted through information technology, such as photos, video, animation, and audio, including electronic material that describes a genital or depicts any act or activity involving a sexual organ or any part of the human body, animal, or object by any means, or other similar pornography that is intended to stimulate sexual desire or cause sexual excitement.	Penalty should be compatible with existing laws in Cambodia. Article 249 on indecent exposure in the Criminal Code subjects a perpetrator to six days to three months of imprisonment and a fine of between one hundred thousand to five hundred thousand Riels. Article 39 of the Law on Suppression of Human Trafficking and Sexual Exploitation punishes persons who distributes pornography to seven days to one month of imprisonment and a fine of between one hundred thousand to two hundred thousand Riels; a person who produces pornography is subject to one month to one year of imprisonment and a fine of between two hundred thousand to two million Riels.	Utilize Article 39 of the Law on Suppression of Human Trafficking and Sexual Exploitation and Article 249 on indecent exposure in the Criminal Code to focus on those offenses.
Article 3: Definition 17. Child pornography refers to any image that is transmitted through information technology, such as photos, video, animation, and audio, including electronic material that describes child pornography or depicts any act or activity involving a sexual organ or any part of the body of a child by any means, or other similar pornography of a child that stimulates sexual desire or causes sexual excitement.	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. Referred to as “child sexual exploitation material” in the draft UN cybercrime treaty. Reference the definition in The Commonwealth Model Law on Computer and Computer Related Crime.	Child pornography shall include pornographic material that visually depicts: a. a minor engaged in sexually explicit conduct; b. a person appearing to be a minor engaged in sexually explicit conduct; c. realistic images representing a minor engaged in sexually explicit conduct

អត្ថបទដើម **Original Text**	យោបល់ និងហេតុផល **Comments and Reasons**	សំណើកែលំអ **Proposal for Improvement**
Article 3: Definition 18. Cryptocurrency is a digital or virtual currency designed to work as a medium of exchange that uses strong cryptography to secure financial transactions and verify the transfer of assets. Cryptocurrencies use decentralized control as opposed to centralized digital currency and central banking systems.	Lack of specificity and clarity may result in a definition so broad as to include commonplace digital payment systems like QR codes. Address this topic through comprehensive cryptocurrency regulation in cooperation with ASEAN cooperation. Reference the definition from the U.S. Department of Commerce National Institute of Standards and Technology (NIST).	Cryptocurrency is a digital asset/credit/unit within the system, which is cryptographically sent from one blockchain network user to another. In the case of cryptocurrency creation (such as the reward for mining), the publishing node includes a transaction sending the newly created cryptocurrency to one or more blockchain network users. These assets are transferred from one user to another by using digital signatures with asymmetric-key pairs.
Article 3: Definition 19. Cybercrime refers to the use of information technology to harm computer systems, computer data, websites, and/or technology, or to harm or commit crimes against individuals or entities, whether directly or indirectly through the use of computer systems, computer data, or information technology.	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. Reference the definition in The Commonwealth Model Law on Computer and Computer Related Crime.	"Cybercrime" is not a defined legal category, but includes: offences aimed at computers, computer or communications systems, their users or the data they contain; and more traditional offences committed using these systems, especially if technologies have significant effects on how the crime is committed or investigated.
Article 5: Competent authority to investigate cybercrime The judicial police officers in charge of anti-cybercrime of the Ministry of Interior's National Police Commissariat are authorized to investigate offenses stipulated in this law. Where necessary, judicial police officers in charge of anti-cybercrime	Privacy and surveillance risks involved with international cooperation. This article may circumvent domestic legal safeguards, oversight mechanisms, and due process protections while undermining the sovereign rights of Cambodians.	Where necessary due to imminent security threats, judicial police officers in charge of the anti-cybercrime unit may collaborate with national or international technical experts to investigate said offenses, provided such collaboration is approved by a court order limiting the time and scope of collaboration, and conducted with appropriate notice to relevant parties unless such notice would jeopardize the investigation.

អត្ថបទដើម **Original Text**	យោបល់ និងហេតុផល **Comments and Reasons**	សំណើកែលំអ **Proposal for Improvement**
may collaborate with national or international technical experts to investigate said offenses.		
Article 7: Competent authority to revoke business rights/business license The competent Ministries or institutions to grant an online business permit, certificate or license may suspend or revoke that business permit, certificate, or license if such online business operator commits an offense as stipulated in this law.	Increases risk level for businesses if inadvertent noncompliance results in a total loss of business license. May deter foreign business entry into the country when combined with Article 18.	A court hearing should be held a decision should be issued by an independent judge before license revocation. Ensure independent review body for appeals. Implement standard due process procedures which will encourages cooperation with authorities to resolve the issue before license is revoked.
Article 10: Confidentiality Service providers shall maintain the confidentiality of computer data, traffic data and subscriber information as stipulated in this law unless authorized by a court order.	Additional detail in this section may be warranted. The cybercrime law should complement the draft cybersecurity law with the goal of enhancing the defensive cybersecurity posture of all technology systems in Cambodia.	Service providers shall maintain the confidentiality of computer data, traffic data and subscriber information by adhering to internationally recognized cybersecurity and encryption standards unless authorized by a court order.
Article 12: Preservation of computer data and traffic data 2. The service providers who are obliged to preserve computer data and/or traffic data as outlined in Paragraph 1 above shall preserve computer data or traffic data for 180 (one hundred and eighty) days. In case of necessity, the competent authority may request an extension	A broad definition of "service providers" may result in very high compliance costs for businesses which would be especially burdensome for SMEs. Some commonplace apps like messaging apps may violate this provision. Proposal for improvement also applies to Article 8, Section 2 and Article 31.	Require data preservation only after a court order. Narrow the definition of Service providers. Account for privacy protection software. Limit to storage requirement to metadata.

អត្ថបទដើម **Original Text**	យោបល់ និងហេតុផល **Comments and Reasons**	សំណើកែលំអ **Proposal for Improvement**
of the data preservation period for one time only for an additional 180 (one hundred and eighty) days.		
Article 12: Preservation of computer data and traffic data 4. The service providers or the persons who own the data as outlined in Paragraph 1 are obliged to effectively preserve such information confidentially and not disclose or take any action that may disclose the preservation of such data to the subscriber or the suspect.	May hinder the transparency reports of multinational corporations that report aggregated statistics on government warrants and requests for personal data. Articles 13 and 15 also have similar wording about disclosure.	4. The service providers or the persons who own the data as outlined in Paragraph 1 are obliged to effectively preserve the confidentiality of such information and should disclose such data to the subscriber, the suspect, or in publicly available transparency reports once the investigation has concluded.
Article 14: Search and seizure of computer data 1. In order to search or gather the evidence necessary for a criminal investigation in which a computer system or a computer data storage medium may contain evidence of that crime, the judicial police officers shall request a court to: - search or access a computer system or part of it and computer data stored therein; - search or access a computer or data storage medium in which computer data may be stored; and - with such assistance as may be	Lack of a minimum threshold or requirement criteria for launching an investigation into a computer system or data storage medium that is thought to contain evidence of a crime. Request improved handling of privileged information since the article doesn't address how to handle potentially privileged or sensitive information. Increase oversight and accountability since the article lacks provisions for independent oversight of search and seizure operations.	Require a judicial police officer to have "probable cause" that a computer system or computer data storage medium contains evidence of a crime before requesting a court to issue a warrant for search and seizure. Clearly describe the surveilled material in the court order request, which must be directly related to the crime being investigated. Limit the duration of the surveillance and require the destruction of the material seized after the investigation concludes. Insert provisions for handling privileged information and ensure independent oversight of search and seizure operations.

អត្ថបទដើម **Original Text**	យោបល់ និងហេតុផល **Comments and Reasons**	សំណើកែលំអ **Proposal for Improvement**
necessary using existing technical capability		
Article 15: Real-time collection of traffic data 2. Upon receiving a written application for an extension by a judicial police officer, it may authorize an extension for a further specified period.	Possibility that judicial police officers could request unlimited extensions for collecting traffic data which would violate principles of privacy and enable excessive surveillance of civil society and the public.	Revise Articles 15(2) and 16(2) to limit extensions of court orders to a maximum of 180 days. Require judicial police officers to demonstrate reasonable grounds to believe that continued access to traffic data and content data would be related to an investigation of a crime.
Article 15: Real-time collection of traffic data 3. This Article shall apply only to investigations related to serious offenses.	Additional specificity and clarity requested for several phrases.	Clearly define "serious offenses" and “national security” that warrant interception. Define “content data”
Article 17: Complaint and transitional fine	Appeals should go to an independent body rather than the Minister of Interior. Cambodian citizens and corporations may find remedies to be insufficient.	Establishing an independent review body for initial appeals. Develop consistent review criteria and procedures.
Article 18: Complaint against the revocation of business rights	Increases risk level for businesses if inadvertent noncompliance results in a total loss of business license. This may deter foreign business entry into the country when combined with Article 7.	A court hearing should be held a decision should be issued by an independent judge before license revocation. Ensure independent review body for appeals. Implement standard due process procedures which will encourages cooperation with authorities to resolve the issue before license is revoked.
Article 22: Transitional Penalty - Cybercrime punishable by transitional penalty shall be determined by sub-decree. - The payment of a transitional fine shall extinguish criminal actions.	Discrimination based on economic status may disproportionately harm those with less wealth.	Tailor the fine to the severity of the offense and the income level of the offender. Allow appeal of transitional fine via independent judicial body before payment is due.

អត្ថបទដើម **Original Text**	យោបល់ និងហេតុផល **Comments and Reasons**	សំណើកែលំអ **Proposal for Improvement**
Article 24: Criminal Liability of Legal Entities A legal entity may be declared criminally liable for an offense committed by an organization or its representative for the benefit of that legal entity as stated in Article 42 (Criminal Liability of legal entities) of the Criminal Code.	Additional specificity and clarity requested for the phrase "for the benefit of that legal entity"	Define "for the benefit of that legal entity"
Article 26: Illegal data distribution by competent officers Any competent officer under this law who intentionally, without lawful authorization, excuse or justification, distributes computer data, traffic data, or other data of the person under investigation shall be punishable by a term of imprisonment from 1 (one) month to 6 (six) months and a fine from 2,000,000 (two million) to 8,000,000 (eight million) Riels.	Privacy concerns about sharing sensitive information about an individual or entity under investigation. Additional specificity and clarity requested for the phrase "excuse of justification"	Adding provisions for justified unauthorized use in the event of public interest (Whistleblower protection). Implement burden of proof standard and appeals process before competent officer can distribute data about entity under investigation.
Article 32: Cryptocurrency Any person who advertises and mobilizes funds for purchase, sale, exchange or payment transactions of cryptocurrency via information technology without authorization or license from the competent authority shall be punishable by a term of imprisonment from 6 (six)	Address this issue through comprehensive cryptocurrency regulation preferably in coordination with ASEAN. See Singapore's Payment Services Act (PSA), Securities and Futures Act (SFA), and Monetary Authority of Singapore as an example. This regulation may have an impact on the banking sector since one cryptocurrency, Ripple (XRP), is commonly used by large banks for cross-border settlements.	Address through comprehensive cryptocurrency regulation or new cryptocurrency law.

អត្ថបទដើម **Original Text**	យោបល់ និងហេតុផល **Comments and Reasons**	សំណើកែលំអ **Proposal for Improvement**
months to 3 (three) years and a fine from 10,000,000 (ten million) to 50,000 000 (fifty million) Riels. Legal entities who violate the above paragraph shall be fined from 200,000,000 (two-hundred million) to 800,000,000 (eight-hundred million) Riels and any additional penalties as stated in Article 24 of this law.		
Article 33: Misrepresentation by service provider Service providers who, through the use of information technology, make misrepresentation about their services for the purpose of exploiting users shall be punishable by a term of imprisonment from 6 (six) months to 3 (three) years and a fine from 10,000,000 (ten million) to 50,000 000 (fifty million) Riels. Legal entities who violate the above paragraph shall be fined from 100,000,000 (one-hundred million) to 500,000,000 (five-hundred million) Riels and any additional penalties as stated in Article 24 of this law.	Broad definition of service provider calls for additional specificity and clarity requested for several phrases.	Define “misrepresentation” and “exploiting users”
Article 34: Unauthorized access	This article could inadvertently criminalize some forms of legitimate system administration, security testing, or research activities.	Add a provision for justified unauthorized use in the event of public interest (Whistleblower protection). Utilize the three-part test for

អត្ថបទដើម **Original Text**	យោបល់ និងហេតុផល **Comments and Reasons**	សំណើកែលំអ **Proposal for Improvement**
		freedom of expression and freedom of information restrictions. Add an exception for good faith security research.
Article 35: Violation of authorized access	This article doesn't consider the sensitivity or classification of the data accessed. There are no provisions for situations where unauthorized use might be justified such as emergencies or whistleblowing.	Add a provision for justified unauthorized use in the event of public interest (Whistleblower protection). Utilize the three-part test for freedom of expression and freedom of information restrictions.
Article 36: Unauthorized data interception	This article could inadvertently criminalize some forms of legitimate system administration, security testing, or research activities. See U.S. Department of Justice prosecutorial guidelines for the Computer Fraud and Abuse Act (CFAA).	Add an exception for good faith security research. “Good faith security research” means accessing a computer solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in a manner designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices, machines, or online services to which the accessed computer belongs, or those who use such devices, machines, or online services. Security research not conducted in good faith—for example, for the purpose of discovering security holes in devices, machines, or services in order to extort the owners of such devices, machines, or services—might be called “research,” but is not in good faith.
Article 37: Illegal computer program or device	This article could inadvertently criminalize some forms of legitimate system administration, security testing, or research activities. See U.S. Department of Justice prosecutorial guidelines for the	Add an exception for good faith security research. “Good faith security research” means accessing a computer solely for purposes of good-faith testing, investigation, and/or

អត្ថបទដើម **Original Text**	យោបល់ និងហេតុផល **Comments and Reasons**	សំណើកែលំអ **Proposal for Improvement**
	Computer Fraud and Abuse Act (CFAA).	correction of a security flaw or vulnerability, where such activity is carried out in a manner designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices, machines, or online services to which the accessed computer belongs, or those who use such devices, machines, or online services. Security research not conducted in good faith—for example, for the purpose of discovering security holes in devices, machines, or services in order to extort the owners of such devices, machines, or services—might be called "research," but is not in good faith.
Article 38: Computer data interference	This article could inadvertently criminalize some forms of legitimate system administration, security testing, or research activities. See U.S. Department of Justice prosecutorial guidelines for the Computer Fraud and Abuse Act (CFAA).	Add an exception for good faith security research. "Good faith security research" means accessing a computer solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in a manner designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices, machines, or online services to which the accessed computer belongs, or those who use such devices, machines, or online services. Security research not conducted in good faith—for example, for the purpose of discovering security holes in devices, machines, or services in

អត្ថបទដើម **Original Text**	យោបល់ និងហេតុផល **Comments and Reasons**	សំណើកែលំអ **Proposal for Improvement**
		order to extort the owners of such devices, machines, or services—might be called "research," but is not in good faith.
Article 39: Computer system interference	This article could inadvertently criminalize some forms of legitimate system administration, security testing, or research activities. See U.S. Department of Justice prosecutorial guidelines for the Computer Fraud and Abuse Act (CFAA).	Add an exception for good faith security research. "Good faith security research" means accessing a computer solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in a manner designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices, machines, or online services to which the accessed computer belongs, or those who use such devices, machines, or online services. Security research not conducted in good faith—for example, for the purpose of discovering security holes in devices, machines, or services in order to extort the owners of such devices, machines, or services—might be called "research," but is not in good faith.
Article 42: Information technology-related abuse Any person who intentionally causes intimidation, threat, or abuse to another person by information technology-related means shall be punishable by a term of imprisonment from 1 (one) month to 6 (six) months and a fine	This article could potentially be used to suppress legitimate criticism or dissent without clear definitions and safeguards.	Only make it a crime if the intimidation, threat, or abuse directly leads to a significant physical or emotional harm. At the end of Article 42, insert a clause that explicitly allows for the criticism of government officials, government policies, and other public figures. Include provisions for prompt retraction or correction of false statements as a mitigating factor.

អត្ថបទដើម **Original Text**	យោបល់ និងហេតុផល **Comments and Reasons**	សំណើកែលំអ **Proposal for Improvement**
from 2,000,000 (two million) to 5,000,000 (five million) Riels. In case of causing grievous harm to the victim, the offender shall be punishable by imprisonment from 6 (one) month to 2 (two) years and a fine from 5,000,000 (five million) to 10,000,000 (ten million). Riels.		
Article 43: Defamation Exaggerated claim or insincere blame for any act that harms the honor or reputation of an individual or institution through information technology shall be fined from 2,000,000 (two million) to 10,000,000 Riels. (ten million) Riel. In case this act causes serious harm to the victim, the offender shall be punishable by imprisonment from 1 (one) month to 6 (six) months and a fine from 10,000,000 (ten million) to 20,000,000 (twenty million) Riels.	This article could potentially be used to suppress legitimate criticism or dissent without clear definitions and safeguards. Defamation is already an offense under the Criminal Code of the Kingdom of Cambodia.	In light of the ongoing UN cybercrime treaty negotiations and the overarching principles of legislative prudence in Cambodia, it is proposed that the continued inclusion of this article within the draft law be reconsidered with an inclination towards its excision to ensure coherence with contemporary, multinational legal standards and mitigate any adverse interpretative ramifications. If Article 43 is retained in the draft law, remove imprisonment as a penalty for defamation and instead state that a court may order the accused to issue a correction of a false statement or to pay a fine of one hundred thousand to ten million Riels, depending on the severity of the harm caused by the statement. Also, add in defenses to the crime of defamation, including if the accused made reasonable efforts to ascertain the truth about a matter in the public interest. Finally, require that the "exaggerated claim or insincere blame" under Article 43 be issued with malice or in bad faith.
Article 44: Insults	This article could potentially be used to suppress legitimate criticism or dissent without clear	In light of the ongoing UN cybercrime treaty negotiations and the overarching principles of

អត្ថបទដើម **Original Text**	យោបល់ និងហេតុផល **Comments and Reasons**	សំណើកែលំអ **Proposal for Improvement**
The use of any insulting, derogatory or rude language without imposing blame on any act through information technology shall be fined from 2,000,000 (two million) Riels to 10,000,000 (ten million) Riels. Riel. In case this act causes serious harm to the victim, the offender shall be punishable by imprisonment from 1 (one) month to 6 (six) months and a fine from 10,000,000 (ten million) to 20,000,000 (twenty million) Riels.	definitions and safeguards. Articles 305, 306, 307, 308, and 309 from the Criminal Code of the Kingdom of Cambodia already address this issue.	legislative prudence in Cambodia, it is proposed that the continued inclusion of this article within the draft law be removed with an inclination towards its excision to ensure coherence with contemporary, multinational legal standards and mitigate any adverse interpretative ramifications.
Article 45: Intellectual property rights (IPR) Any person, without lawful authorization or permission, uses information technology to distribute, produce or sell intellectual property rights of others shall be punishable by a term of imprisonment from 3 (three) months to 1 (one) year and a fine from 15,000,000 (fifteen million) to 25,000 000 (twenty-five million) Riels. Legal entities who violate the above paragraph shall be fined from 100,000,000 (one-hundred million) to 500,000,000 (five-hundred million) Riels and any additional	Creates an elevated risk for technology companies that face possible imprisonment for accidental IP violations. Raises the possibility that AI companies can be criminally convicted for using the copyrighted content of news websites.	Adjudicate I.P. disputes in civil court rather than via criminal prosecutions. The penalties for violations should be exclusively monetary. Reform existing laws such as the Trademark and Unfair Competition Law, the Law on Patents, Utility Model Certificates, and the Industrial Designs Law on Copyright and Related Rights.

អត្ថបទដើម **Original Text**	យោបល់ និងហេតុផល **Comments and Reasons**	សំណើកែលំអ **Proposal for Improvement**
penalties as stated in Article 24 of this law.		
Article 47: Computer-related forgery Any person, without right, engages in the input, alteration or deletion of computer data or the restriction of the access to such computer data, resulting in inauthentic data, with the intent to be used for legal purposes shall be punishable by a term of imprisonment from 2 (two) years to 5 (five) years and a fine from 10,000,000 (ten million) to 25,000 000 (twenty-five million) Riels.	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. Reference the definition in the draft UN cybercrime treaty.	"Information and communications technology system-related forgery 1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion or suppression of electronic data resulting in inauthentic data with the intent that they be considered or acted upon for legal purposes as if they were authentic, regardless of whether or not the data are directly readable and intelligible. 2. A State Party may require an intent to defraud, or a similar dishonest or criminal intent, before criminal liability attaches."
Article 49: Communication of false information Any person who disseminates or distributes false information through information technology that intentionally harms national defense, national security, relations with other countries, economy, public order, or causes discrimination, or affects traditional culture shall be punishable by imprisonment from 3 (three) years to 5 (five) years and a fine from 50,000,000 (fifty million) to	This article could potentially be used to suppress legitimate criticism or dissent without clear definitions and safeguards.	In light of the ongoing UN cybercrime treaty negotiations and the overarching principles of legislative prudence in Cambodia, it is proposed that the continued inclusion of this article within the draft law be removed with an inclination towards its excision to ensure coherence with contemporary, multinational legal standards and mitigate any adverse interpretative ramifications.

អត្ថបទដើម **Original Text**	យោបល់ និងហេតុផល **Comments and Reasons**	សំណើកែលំអ **Proposal for Improvement**
100,000,000 (one-hundred million) Riels. Legal entities who violate the above paragraph shall be fined from 200,000,000 (two-hundred million) to 500,000,000 (five-hundred million) Riels and any additional penalties as stated in Article 24 of this law.		
Article 50: Attempt An attempt to commit an offense through information technology shall be subject to the same penalties for that enumerated offense as stipulated in this law.	Mere attempt can be too low bar to potentially implicate an entity in a criminal offense. A futile attempt would potentially face the same punishment as an offense that was completed.	Add requirement for "dangerous proximity" or a "substantial step" towards the offense.
Article 51: Conspiracy Participating in a group or a conspiracy established with a view to committing an offense through information technology shall be subject to the same penalties for that enumerated offense as stipulated in this law.	Conspiracy can be overinclusive and include individuals not intending to contribute to the offense. May not even require an overt act by an entity.	Request to remove this article