ISSN 1560-7615 / ISBN 978-99950-52-06-5

ឯកសារបោះពុម្ពផ្សាយរបស់
វិទ្យាស្ថានបណ្តុះបណ្តាល និង ស្រាវជ្រាវដើម្បីអភិវឌ្ឍន៍កម្ពុជា

ធនធានដើម្បីអភិវឌ្ឍន៍កម្ពុជា

ឆ្នាំទី ២៣ ២០១៩
តម្លៃ ១.៥០០រ

30 ANNIVERSARY CDRI 1990 - 2020

អភិបាលកិច្ចសន្តិសុខអ៊ុនធើណិតនៅកម្ពុជា៖ ស្ថានភាពបច្ចុប្បន្ន និងអនាគត

សេចក្តីផ្តើម

អត្ថបទនេះពិភាក្សាពីបញ្ហាសុវត្ថិភាពអ៊ុនធើណិត បទល្មើសតាមអ៊ុនធើណិត និងអភិបាលកិច្ចសន្តិសុខអ៊ុនធើណិត ដោយពិនិត្យឡើងវិញពីគោលនយោបាយ និងប្រព័ន្ធអភិបាលកិច្ចនាពេលបច្ចុប្បន្ននៅកម្ពុជា និងនៅប្រទេសអាស៊ានដទៃទៀត ព្រមទាំងធ្វើការវាយតម្លៃពីយុទ្ធសាស្ត្រ និងផែនការរបស់ក្រសួងនានា មជ្ឈមណ្ឌលស្រាវជ្រាវ និងក្រុមហ៊ុនអន្តរជាតិធំៗ។

ប្រទេសកម្ពុជាកំពុងខិតខំពង្រឹងអភិបាលកិច្ចសន្តិសុខតាមអ៊ុនធើណិត ដើម្បីកាត់បន្ថយហានិភ័យដែលអាចកើតមានពីទំនាក់ទំនងសកលកាន់តែខ្លាំងឡើង ខែតុលា ឆ្នាំ២០១៩

បុគ្គល ស្ថាប័នរដ្ឋ និងអង្គការនានា កាន់តែពឹងផ្អែកខ្លាំងឡើង ទៅលើប្រព័ន្ធអេកូបច្ចេកវិទ្យាសុគស្មាញ ដើម្បីប្រាស្រ័យទាក់ទង និងធ្វើអន្តរកម្មជាមួយអ្នកមានជំនាញដូចគ្នា ដៃគូអាជីវកម្ម និងអតិថិជន, ចែករំលែក និងទទួលបានព័ត៌មាន, ផ្តល់ទិន្នន័យ សម្រាប់កែលំអការសម្រេចចិត្ត និងលទ្ធផល, និងបង្កើនលទ្ធភាពឈោងដល់ និងផលចំណេញ។ ប្រព័ន្ធបច្ចេកវិទ្យាឌីជីថល កាន់តែចាំបាច់ឡើងទៀតក្នុងពេលមានជំងឺឆ្លងរាលដាលដូច កូវីដ១៩ នាពេលបច្ចុប្បន្ន។ ក្នុងពេលជាមួយគ្នា ការវាយប្រហារតាមអ៊ុនធើណិត បានកើតមានឡើងកាន់តែញឹកញាប់ និងធ្ងន់ធ្ងរ។ ទាំងបុគ្គលឯកជន អ្នកនយោបាយ សមាជិកក្រុមប្រឹក្សាភិបាល និងអ្នកគ្រប់គ្រងអង្គភាព កាន់តែបានដឹងច្បាស់ថា នវានុវត្តន៍ផ្អែកលើបច្ចេកវិទ្យា និងគំនិតផ្តួចផ្តើមផ្សេងៗ វាបើកច្រកនាំឲ្យមានហានិភ័យតាមអ៊ុនធើណិត និងបញ្ហាប្រឈមកាន់តែធំផ្អែកអភិបាលកិច្ច។

ដោយសារវាជាប្រធានបទថ្មីសម្រាប់កម្ពុជា ការសិក្សានេះមានគោលដៅលើកកម្ពស់ចំណាប់អារម្មណ៍ និងបំផុសកិច្ចសន្ទនាដ៏មានប្រយោជន៍ តាមការសម្រួលឲ្យលទ្ធផលស្រាវជ្រាវបានជ្រាបទៅដល់អ្នកកសាងនយោបាយ មន្ត្រីរដ្ឋាភិបាល និងអ្នកដឹកនាំសហគ្រាស សម្រាប់ការកសាងយុទ្ធសាស្ត្រ និងការបង្កើតនិងកែលំអក្របខ័ណ្ឌសន្តិសុខអ៊ុនធើណិតរបស់ខ្លួន (ពោលគឺ អភិបាលកិច្ច បច្ចេកវិទ្យា សមត្ថភាព និងសហប្រតិបត្តិការ)។ អ្នកនិពន្ធសង្ឃឹមថា អ្នកស្រាវជ្រាវ និងអ្នកអនុវត្តជាក់ស្តែង អាចជួយពង្រីកលទ្ធផលរកឃើញទាំងនេះ និងតាមទាន់បច្ចេកវិទ្យាថ្មីៗ និងការផ្លាស់ប្តូរបច្ចេកវិទ្យាយ៉ាងលឿននៅកម្ពុជា។

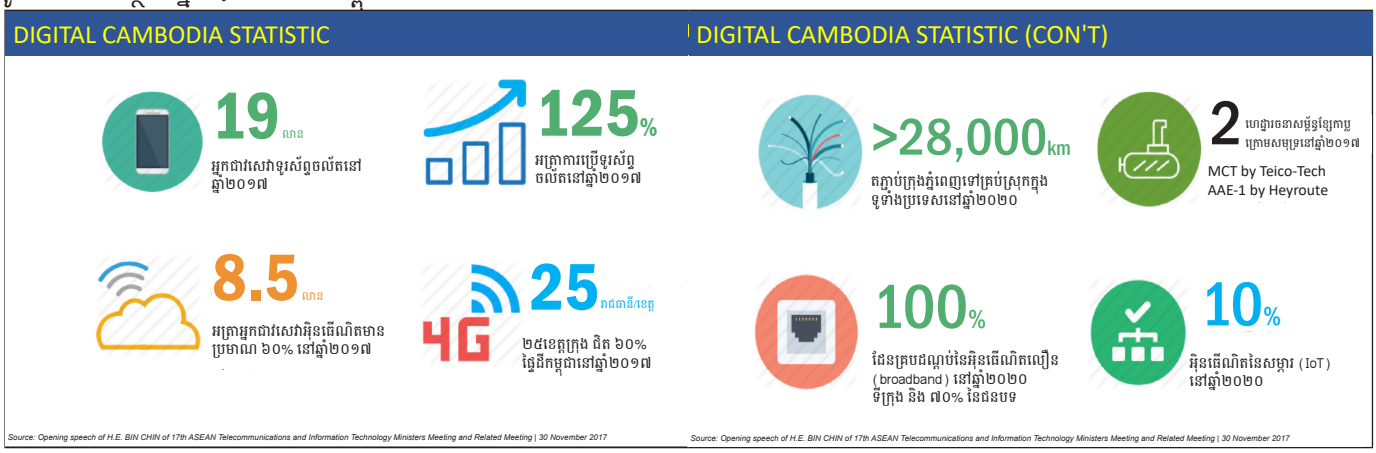
សន្តិសុខអ៊ុនធើណិតនៅកម្ពុជា និងនៅក្នុងសកលលោក

កម្ពុជាមានសេដ្ឋកិច្ចកើនឡើងយ៉ាងលឿន ដល់ ៧,៥% នៅឆ្នាំ២០១៨ (World bank 2019) ពោលគឺកើនឡើងលឿន

មាតិកា

សូមយោងអត្ថបទនេះថា៖ A CDRI Publication. 2019. “Cybergovernance in Cambodia: Current State and Future Priorities.” *Cambodia Development Review* vol. 23, 2019: 1–6។

រូបភាព១៖ ស្ថិតិផ្នែកឌីជីថលនៅកម្ពុជា



ប្រភព៖ Ou 2018 (តាមការអនុញ្ញាតពីអ្នកនិពន្ធ)

បំផុតក្នុងតំបន់អាស៊ាន និងស្ថិតក្នុងចំណោមប្រទេសមានសេដ្ឋកិច្ចកើនឡើងលឿនបំផុតក្នុងពិភពលោក។ ទន្ទឹមនឹង កំណើនសេដ្ឋកិច្ចគួរកោតសរសើរនេះ ស្ថាប័នរដ្ឋ ក្រុមហ៊ុន និងអង្គការនានានៅកម្ពុជា កំពុងពង្រីកការប្រើប្រាស់បច្ចេកវិទ្យាយ៉ាងលឿន (រូបភាព១)។ កំណើនការប្រើប្រព័ន្ធឌីជីថលនេះ ជំរុញឡើងជាសំខាន់ ដោយសារប្រជាជនកម្ពុជាមួយភាគធំមានវ័យក្មេង ពោលគឺ មានអាយុមធ្យម (median age) ត្រឹម ២៥,៦ឆ្នាំ។

ចាប់ពីឆ្នាំ២០១៧ ដល់ ២០១៩ ចំនួនអ្នកប្រើប្រាស់បណ្តាញសង្គមកើន ៧១% ពី ៤,៩លាននាក់ ដល់ ៨,៤លាននាក់ គឺជិតដល់ពាក់កណ្តាលនៃប្រជាជនសរុប (Kepios Analysis 2019)។ ស្ថិតិទាំងនេះ បង្ហាញពី ស្ថានភាពល្អក្នុងប្រទេសទាំងមូលក៏ពិតមែន ប៉ុន្តែការជឿនលឿនយ៉ាងឆាប់រហ័សខាងផ្នែកបច្ចេកវិទ្យាបែបនេះមែន អាចធ្វើឲ្យកម្ពុជាងាយរងគ្រោះដោយសារការវាយប្រហារតាមអ៊ិនធើណិត បើសិនពុំមានការកែលំអក្របខ័ណ្ឌសន្តិសុខអ៊ិនធើណិតនោះទេ។ ជនល្មើសតាមអ៊ិនធើណិត កំពុងប្រើប្រាស់ឧបករណ៍កាន់តែទំនើប និងងាយពង្រីកថែម ដើម្បីជ្រៀតចូលយកព័ត៌មានផ្ទាល់ខ្លួនរបស់អ្នកប្រើអ៊ិនធើណិត ហើយពួកវាសម្រេចបានលទ្ធផលមួយចំនួន។

ជនល្មើសតាមអ៊ិនធើណិត (បុគ្គលឯកជន អ្នកសកម្មវាយលុក និង/ឬ ជនល្មើសមានរដ្ឋជួយឧបត្ថម្ភ) តែងផ្តោតលើតំណ (link) ខ្សោយបំផុតក្នុងអ៊ិនធើណិត ពោលគឺ តាមធម្មតាក្រុមហ៊ុនធំៗតែងរងគ្រោះច្រើនពីការវាយប្រហារតាមអ៊ិនធើណិត ដែលត្រូវបានអនុវត្តឡើងឆ្លងតាម ដៃគូជាភាគីទី៣ អ្នកផ្គត់ផ្គង់ និងអ្នកលក់នៅក្នុងខ្សែសង្វាក់ផ្គត់ផ្គង់របស់ក្រុមហ៊ុន។

តម្រូវការឲ្យមាន ក្របខ័ណ្ឌអភិបាលកិច្ចសន្តិសុខអ៊ិនធើណិត គឺមាន គេយល់ស្របកាន់តែច្រើនឡើងហើយថាជាទិដ្ឋភាពសំខាន់មួយ នៃការកាត់បន្ថយហានិភ័យតាមប្រព័ន្ធអ៊ិនធើណិត។ សន្តិសុខអ៊ិនធើណិត រួមទាំង អភិបាលកិច្ចសន្តិសុខអ៊ិនធើណិតផង ជាអាទិភាពទី៦ ក្នុងចំណោមអាទិភាពសកលទាំង ១០ សម្រាប់ឆ្នាំ២០១៩ ពោលគឺ ខ្ពស់ជាងអាទិភាពនៃការប្រយុទ្ធប្រឆាំងនឹងអំពើភេរវកម្មឆ្លងប្រទេស និង ការលើកកម្ពស់សុខភាពសកលទៅទៀត និងស្ថិតក្នុងចំណោម បញ្ហាប្រឈមផ្នែកគោលនយោបាយបន្ទាន់ៗជាងគេក្នុងពិភពលោក។

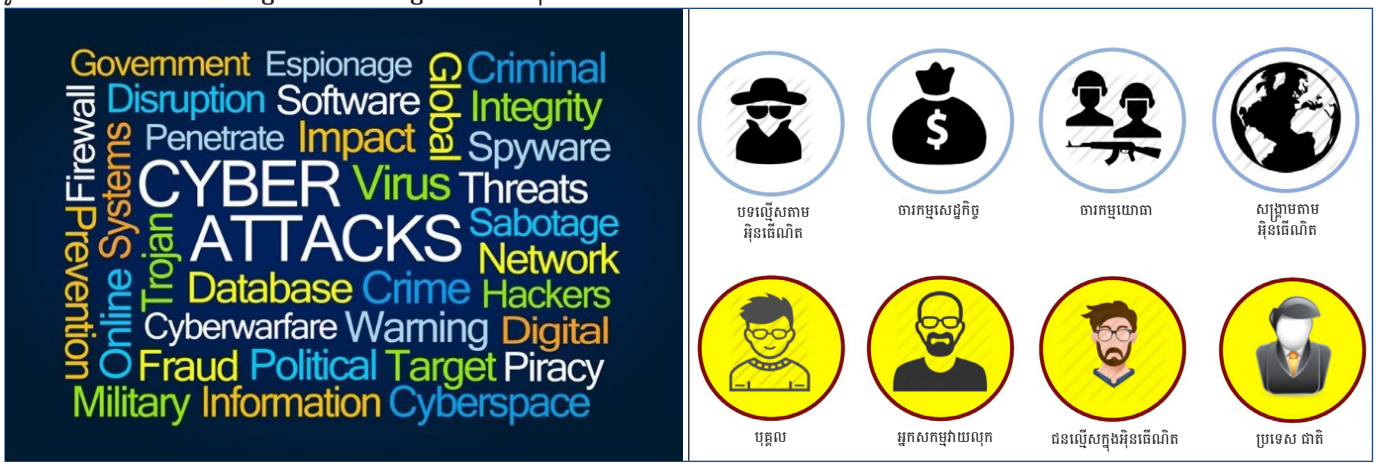
ក្របខ័ណ្ឌអភិបាលកិច្ចសន្តិសុខអ៊ិនធើណិតនៅកម្ពុជា

យ៉ាងហោចណាស់ក្នុងទ្រឹស្តីដែរ ក្របខ័ណ្ឌសន្តិសុខអ៊ិនធើណិត រួមមាន អភិបាលកិច្ច (ច្បាប់ សមត្ថភាពបច្ចេកទេស ការដឹកនាំ) បច្ចេកវិទ្យា (សមត្ថភាពបច្ចេកទេស និងស្ថាប័ន) និង ប្រតិបត្តិការ (ការកសាងសមត្ថភាព សហប្រតិបត្តិការ និងភាពជាដៃគូ) ព្រមទាំង តួអង្គសំខាន់ៗ ដូចជា មន្ទីរក្រសួងរដ្ឋ តុលាការ ស្ថាប័នពង្រឹងអនុវត្តច្បាប់ សហគមន៍ស៊ើបការណ៍ម្ចាស់ និងប្រតិបត្តិករហេដ្ឋារចនាសម្ព័ន្ធសំខាន់ៗ អ្នកលក់ដូរ អ្នកសិក្សាអប់រំ ពលរដ្ឋ និង អ្នកពាក់ព័ន្ធបរទេស។

នៅពេលអ្នកនិពន្ធកំពុងតាក់តែងអត្ថបទនេះ គឺមានសេចក្តីព្រាងច្បាប់ថ្មីមួយស្តីពី បទល្មើសតាមអ៊ិនធើណិត ដែលត្រូវបានលើកយកមកពិភាក្សានៅក្រសួងមហាផ្ទៃ ហើយគេរំពឹងថានឹងមានការកែប្រែជាច្រើនទៀត នៅក្នុងសេចក្តីព្រាងច្បាប់ដំបូងឆ្នាំ២០១៤ នេះ ។ ដោយសារសេចក្តីព្រាងច្បាប់ចុងក្រោយមិនទាន់មានការផ្សព្វផ្សាយជាសាធារណៈ ដូច្នេះការវិភាគនៅខាងក្រោមផ្អែកលើសេចក្តីព្រាងច្បាប់ឆ្នាំ២០១៤ (ជាភាសាខ្មែរ និងអង់គ្លេស) ដែលមិនទាន់ផ្លូវការនៅឡើយ។

គោលដៅនៃ សេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសតាមអ៊ិនធើណិត ឆ្នាំ២០១៤ គឺដើម្បីប្រយុទ្ធប្រឆាំងនឹងបទល្មើសផ្សេងៗដែលអនុវត្តឡើងតាមប្រព័ន្ធកុំព្យូទ័រ (ឧបករណ៍មួយ ឬ ឧបករណ៍តភ្ជាប់គ្នាមួយខ្សែ) និងដើម្បីការពារ និងធានាសុវត្ថិភាពសិទ្ធិស្របច្បាប់ និងផលប្រយោជន៍របស់នីតិបុគ្គល និងរូបវន្តបុគ្គលនិងរបស់ប្រទេសកម្ពុជា។ ក្នុងនេះរដ្ឋាភិបាលបានបង្កើតគណៈកម្មាធិការជាតិប្រឆាំងនឹងបទល្មើសតាមអ៊ិនធើណិត (NACC) ដែលមាននាយករដ្ឋមន្ត្រីជាប្រធាន ដើម្បីកសាងយុទ្ធសាស្ត្រផែនការសកម្មភាព និងវិធានការជាប់ទាក់ទិនផ្សេងៗខាង

រូបភាព២៖ ភាពងាយរងគ្រោះពីការវាយប្រហារតាមអ៊ិនធើណិត



ប្រភព៖ Ou 2018 (តាមការអនុញ្ញាតពីអ្នកនិពន្ធ)

សន្តិសុខអ៊ិនធើណិត និងប្រព័ន្ធព័ត៌មាន សម្រាប់រដ្ឋាភិបាល។ ច្បាប់នេះក៏បានផ្តល់អំណាច "គោលនយោបាយតុលាការ" ដល់អគ្គនាយក និងអគ្គនាយករង នៃលេខាធិការដ្ឋាន NACC ដើម្បីធ្វើការឃាត់ខ្លួន និងស៊ើបអង្កេតលើសកម្មភាពរបស់ជនជាប់សង្ស័យ (មាត្រា១៥)។

សរុបមកខ្លឹមសារនៃសេចក្តីព្រាងច្បាប់នេះ សំដៅដោះស្រាយការព្រួយបារម្ភអំពី បទល្មើសធម្មតាតាមអ៊ិនធើណិត ដូចជា ការលួចចូលខុសច្បាប់ ចារកម្មទិន្នន័យ ការលួចកម្មសិទ្ធិបញ្ញាជាដើម ដោយមានការកំណត់ទោសទ័ណ្ឌ សម្រាប់បទល្មើសនីមួយៗ។ ប៉ុន្តែនៅមានបញ្ហាចោទជាច្រើនទៀត ជាពិសេសទាក់ទងនឹងមាត្រា២៨ ដែលអាចរឹតត្បិតសិទ្ធិសេរីភាពក្នុងការបញ្ចេញមតិ។ ឧទាហរណ៍ កថាខ័ណ្ឌ៤ នៃមាត្រា២៨ ចែងថា ការផ្សព្វផ្សាយព័ត៌មានមិនពិតអំពីរដ្ឋាភិបាល ជាបទល្មើសអាចផ្តន្ទាទោសតាមច្បាប់។ ប៉ុន្តែក្នុងនោះ រដ្ឋាភិបាល គឺជាអ្នកកំណត់ថា ការផ្សព្វផ្សាយណាមួយជា "ព័ត៌មានមិនពិត"។

ដោយសារបទល្មើសតាមអ៊ិនធើណិត មានលក្ខណៈបន្ទាន់ស្មុគស្មាញ និងប៉ះពាល់ដល់គ្រប់ទិដ្ឋភាពសង្គម ដូច្នេះបទបញ្ញត្តិស្តីពីបទល្មើសតាមអ៊ិនធើណិត ត្រូវមានកិច្ចប្រឹងប្រែងដោយរួមសហការគ្នារវាង វិស័យសាធារណៈ វិស័យឯកជន និង វិស័យសិក្សាអប់រំ។

លទ្ធផលរកឃើញសំខាន់ៗ និងការផ្តល់មតិ

ចំណុចខ្លះខាតសំខាន់ៗ បួន បានលេចចេញពីការវិភាគលើកិច្ចប្រឹងប្រែងផ្នែកអភិបាលកិច្ចសន្តិសុខអ៊ិនធើណិត និងការជំរុញកិច្ចប្រឹងប្រែងនេះ គឺមាន៖

- តម្លាភាពរបស់រដ្ឋាភិបាល
- ធនធានមនុស្ស និងបច្ចេកទេស
- កិច្ចសហការក្នុងតំបន់
- គោលដៅជាក់ស្តែងអាចវាស់វែងបាន

ការផ្តល់មតិទី១៖ កម្ពុជាកំពុងស្ថិតក្នុងដំណាក់កាលដំបូងនៃការកសាងក្របខ័ណ្ឌសន្តិសុខអ៊ិនធើណិតរបស់ខ្លួន ដោយប្រឹងដោះស្រាយចំណុចខ្វះខាតសំខាន់ៗទាំងបួនខាងលើ ជាពិសេសក្នុងបញ្ហា តម្លាភាព និង កិច្ចការពារសិទ្ធិមនុស្ស និងផលប្រយោជន៍ជាតិ, ការកសាងកម្លាំងពលកម្មមានជំនាញខ្ពស់សម្រាប់ប្រើប្រាស់បច្ចេកវិទ្យាឌីជីថលនាពេលអនាគត, និងការបង្កើតភាពជាដៃគូជាយុទ្ធសាស្ត្រជាមួយប្រទេសដទៃទៀត និងក្រុមហ៊ុនអន្តរជាតិនានា។ ក្នុងស្ថានភាពបច្ចុប្បន្ន ជាប្រទេសកំពុងអភិវឌ្ឍ កម្ពុជានៅមានឧបសគ្គធំៗត្រូវដោះស្រាយមួយរយៈពេលទៀត ប៉ុន្តែការប្រើប្រាស់របៀបរបបអន្តរជាតិល្អៗដូចជា ស្តង់ដា និងក្របខ័ណ្ឌផ្សេងៗជាដើម អាចជួយកម្ពុជាក្នុងការដាក់អនុវត្តប្រព័ន្ធមានប្រសិទ្ធភាព និងដំណើរការបានល្អ ដើម្បីការពារហេដ្ឋារចនាសម្ព័ន្ធ នៃបច្ចេកវិទ្យាគមនាគមន៍និងព័ត៌មាន (ICT) របស់ខ្លួន និងអ្នកប្រើប្រាស់ អំពីការវាយប្រហារតាមអ៊ិនធើណិត។

ក្នុងចក្ខុវិស័យ ដើម្បីក្លាយជាប្រទេសអភិវឌ្ឍន៍ពេញលេញនៅឆ្នាំ២០៥០ (Seangly 2013) កម្ពុជាបានកំណត់គោលដៅប្រកបដោយមហិច្ឆតាជាច្រើន មានជាអាទិ៍ ការធ្វើវិនិយោគយ៉ាងច្រើនក្នុងការកសាងហេដ្ឋារចនាសម្ព័ន្ធឌីជីថល ការអភិវឌ្ឍទីក្រុងឆ្លាត និងការអនុវត្តតាមគោលការណ៍នៃឧស្សាហកម្ម ៤.០ នៅក្នុងកម្មន្តសាលកម្ម។ ការវាយប្រហារទ្រង់ទ្រាយធំ តាមអ៊ិនធើណិត ទៅលើបច្ចេកវិទ្យាទាំងនេះមុនពេលវាអនុវត្តបានពេញលេញ និងមានសន្តិសុខល្អ អាចបង្កឧបសគ្គធ្ងន់ធ្ងរដល់ប្រសិទ្ធភាពនិងការរីកចម្រើនរបស់វា ហើយតាមនេះអាចបង្កផលលំបាកដោយផ្ទាល់ដល់កំណើនសេដ្ឋកិច្ចកម្ពុជា។

ការផ្តល់មតិទី២៖ កិច្ចការពារហេដ្ឋារចនាសម្ព័ន្ធសំខាន់ៗ ដូចជា សុខភាពសាធារណៈ ការដឹកជញ្ជូន ប្រព័ន្ធទូរគមនាគមន៍ និងការផ្គត់ផ្គង់ទឹក និងអគ្គិសនី គឺជាទំនួលខុសត្រូវចម្បងរបស់

រដ្ឋាភិបាល ហើយគួរដោះស្រាយតាមការរួមដៃគ្នា ជាធ្លុងមួយ រវាងវិស័យសាធារណៈ វិស័យឯកជន និងវិស័យសិក្សាអប់រំ។

ការផ្តល់មតិទី៣៖ ច្បាប់ និងបទបញ្ញត្តិស្តីពីសន្តិសុខអ៊ិនធើណិត ត្រូវតែអនុម័តចេញ។ ឧទាហរណ៍យ៉ាងល្អមួយនៃច្បាប់សន្តិសុខអ៊ិនធើណិតដែលត្រូវបានគ្រោងឡើងយ៉ាងហ្មត់ចត់ គឺច្បាប់សន្តិសុខអ៊ិនធើណិតឆ្នាំ២០១៨ របស់សិង្ហបុរី។ ច្បាប់នេះបានចែងយ៉ាងលំអិត និងច្បាស់ៗថា អង្គការជាប់ពាក់ព័ន្ធនឹងហេដ្ឋារចនាសម្ព័ន្ធសំខាន់ៗនៅសិង្ហបុរីមួយណាត្រូវធ្វើអ្វីខ្លះ និងបានកំណត់ច្បាស់ថា រដ្ឋាភិបាលអាចធ្វើអ្វី និងមិនអាចធ្វើអ្វី ក្នុងការការពារសន្តិសុខជាតិ (Republic of Singapore 2018)។ ជាជាងសេចក្តីចែងមិនសូវច្បាស់ពី បទល្មើស និងតុល្យភាពអំណាច ច្បាប់សន្តិសុខអ៊ិនធើណិតរបស់សិង្ហបុរី បានផ្តោតលើការធានា ឲ្យមានសហប្រតិបត្តិការ និងតម្លាភាពរវាងវិស័យសាធារណៈ និងវិស័យឯកជន។

ច្បាប់ស្តីពីសន្តិសុខអ៊ិនធើណិត គួរផ្តោតលើការទប់ស្កាត់ និងការឆ្លើយតបនឹងការវាយប្រហារតាមអ៊ិនធើណិតដោយប្រើបច្ចេកទេសខ្ពស់ ទៅលើ ហេដ្ឋារចនាសម្ព័ន្ធ រដ្ឋាភិបាល និងអាជីវកម្មនានា ព្រោះផលប៉ះពាល់របស់វាទៅលើសេដ្ឋកិច្ចកម្ពុជា អាចធំធេងខ្លាំងជាង បទល្មើស និងការចាត់ទុកជាជនល្មើសច្បាប់

សម្រាប់កម្ពុជា ច្បាប់ស្តីពីសន្តិសុខអ៊ិនធើណិត គួរផ្តោតលើការទប់ស្កាត់ និងការឆ្លើយតបនឹងការវាយប្រហារ តាមអ៊ិនធើណិតដោយប្រើបច្ចេកទេសខ្ពស់ ទៅលើ ហេដ្ឋារចនាសម្ព័ន្ធ រដ្ឋាភិបាល និងអាជីវកម្មនានា ព្រោះផលប៉ះពាល់របស់វា ទៅលើសេដ្ឋកិច្ចកម្ពុជា អាចធំធេងខ្លាំងជាងបទល្មើស និងការចាត់ទុក ជាជនល្មើសច្បាប់ ដោយសារតែការផ្សព្វផ្សាយព័ត៌មានដែលជាចំណុចផ្តោតនៃសេចក្តីព្រាងច្បាប់ ស្តីពី បទល្មើសតាមអ៊ិនធើណិតឆ្នាំ២០១៨ ទៅទៀត។

ការផ្តល់មតិទី៤៖ ការកសាងកម្មវិធីអភិបាលកិច្ច និងសន្តិសុខអ៊ិនធើណិត ឲ្យទៅជាក្របខ័ណ្ឌសន្តិសុខអ៊ិនធើណិត វាស្មុគស្មាញជាខ្លាំង ព្រោះជាប់ទាក់ទងដល់គ្រប់ឧស្សាហកម្ម និងរបៀបរបបរស់នៅ និងជាប់ពាក់ព័ន្ធដល់អាជ្ញាធរគ្រប់កម្រិត ហើយអាចមានផលប៉ះពាល់ផ្នែកហិរញ្ញវត្ថុដោយផ្ទាល់ដល់សេដ្ឋកិច្ច និងសង្គម។ តាមនេះរដ្ឋាភិបាលគួរពិចារណាលើសកម្មភាពដូចតទៅ ក្នុងការកសាងកម្មវិធី អភិបាលកិច្ចសន្តិសុខអ៊ិនធើណិតរបស់ខ្លួន៖ យុទ្ធសាស្ត្រជាតិ ដើម្បីការពារហេដ្ឋារចនាសម្ព័ន្ធសំខាន់ៗ កិច្ចសហការរវាងវិស័យសាធារណៈនឹងឯកជន បទបញ្ញត្តិគ្រប់គ្រងសន្តិសុខអ៊ិនធើណិត ការអនុម័តប្រើស្តង់ដាសន្តិសុខអ៊ិនធើណិតមួយចំនួន ការចែករំលែកព័ត៌មានក្នុងតំបន់ ការលើកកម្ពស់ការយល់ដឹងរបស់សហគមន៍ និង ការកសាងសមត្ថភាព។ សកម្មភាពនីមួយៗដូចខាងលើនេះ តំណាងឲ្យគម្រោងមួយ ដែលគួរមានការត្រួតពិនិត្យជាប់រហូតលើការជឿនលឿនទៅមុន និងលទ្ធផលបានវាស់វែងជាក់លាក់ ពីសំណាក់អាជ្ញាធរអភិបាលកិច្ចសន្តិសុខអ៊ិនធើណិតថ្នាក់ជាតិមួយ (NACC) ដែលមានសមាសភាពមកពីខាង រដ្ឋាភិបាល អាជីវកម្មសំខាន់ៗ និងភាគីពាក់ព័ន្ធមិនមែនរដ្ឋាភិបាលផ្សេងៗ ហើយអាជ្ញាធរនេះមានទំនួលខុសត្រូវតែមួយគត់គឺ ធានាភាពធន់នៃប្រព័ន្ធឌីជីថលកម្ពុជា។

សព្វថ្ងៃមាន ស្តង់ដា និងក្របខ័ណ្ឌសន្តិសុខអ៊ិនធើណិតជាច្រើនដែលគេបានទទួលស្គាល់ ហើយដែលគេអាចយកមកប្រើដើម្បីកសាងកម្មវិធីអភិបាលកិច្ចសន្តិសុខអ៊ិនធើណិត។ ក្នុងនេះក្របខ័ណ្ឌសម្រាប់កែលំអសន្តិសុខអ៊ិនធើណិត នៃហេដ្ឋារចនាសម្ព័ន្ធសំខាន់ៗ (NIST 2018) (បង្កើតឡើងដោយ វិទ្យាស្ថានជាតិផ្នែកស្តង់ដា និងបច្ចេកវិទ្យា (NIST) នៅសហរដ្ឋអាមេរិក ដើម្បីឆ្លើយតបនឹងការរីកចម្រើនបច្ចេកវិទ្យាយ៉ាងលឿន និងកំណើនការគំរាមកំហែងលើសន្តិសុខអ៊ិនធើណិត) គឺកំពុងកើនប្រជាប្រិយភាពយ៉ាងលឿន ដោយសារ មានការប្រើវិធីសាស្ត្រផ្អែកលើហានិភ័យ និងការប្រើពាក្យពេចន៍ច្បាស់ៗអាចយល់បាន។ កម្ពុជាគួរស្រង់យកបទពិសោធន៍នេះក្នុងកិច្ចប្រឹងប្រែងរបស់ខ្លួន ដើម្បីពង្រឹងសន្តិសុខ និងភាពធន់នៃហេដ្ឋារចនាសម្ព័ន្ធសំខាន់ៗ របស់ប្រទេសជាតិ និងដើម្បីថែរក្សានូវបរិស្ថានអ៊ិនធើណិតមួយ ដែលលើកទឹកចិត្ត ឲ្យមានប្រសិទ្ធភាពនវានុវត្តន៍ និងការរីកចម្រើនសេដ្ឋកិច្ច ហើយទន្ទឹមគ្នានោះ ក៏ពង្រឹងសុវត្ថិភាព សន្តិសុខ ការរក្សាការសម្ងាត់របស់អាជីវកម្ម ការការពារឯកជនភាពនិងសេរីភាពរបស់ពលរដ្ឋផងដែរ។

ការផ្តល់មតិទី៥៖ ការកសាងកម្មវិធី សន្តិសុខអ៊ិនធើណិត ដោយប្រើគំរូ ដូចជា ក្របខ័ណ្ឌសន្តិសុខ NIST ជាដើម អាចជួយផ្តល់នូវភាសារួមគ្នាមួយ សម្រាប់ការប្រាស្រ័យទាក់ទងគ្នាអំពីហានិភ័យតាមអ៊ិនធើណិតរវាង កម្រិតផ្សេងៗនៃរដ្ឋាភិបាល និងវិស័យផ្សេងៗនៃឧស្សាហកម្ម ដែលត្រួតពិនិត្យលើហេដ្ឋារចនាសម្ព័ន្ធឌីជីថល សំខាន់ៗនៅកម្ពុជា។ ម្យ៉ាងទៀត គោលនយោបាយលើសន្តិសុខអ៊ិនធើណិតនាបច្ចុប្បន្ន ការបណ្តុះបណ្តាល និងដំណោះស្រាយផ្សេងៗ គួរមានកំណត់គោលដៅទៅអនាគត និងផ្តល់អាទិភាពដល់នវានុវត្តន៍ ព្រមទាំងតាមដាននិងផ្សព្វផ្សាយពីដំណើរការជឿនលឿនទៅដល់អ្នកពាក់ព័ន្ធនានា។ កិច្ចការនេះអាចសម្រេចបានតាមការបំបែកសន្តិសុខអ៊ិនធើណិត និងអភិបាលកិច្ច ទៅជាចំណុចសំខាន់ៗសម្រាប់ធ្វើការអភិវឌ្ឍ៖

១. ការកំណត់ទ្រព្យសម្បត្តិ ដើម្បីឲ្យមានបរិបទច្បាស់សម្រាប់ការស្វែងយល់ពីហានិភ័យតាមអ៊ិនធើណិត
២. ការការពារទ្រព្យសម្បត្តិដោយដាក់អនុវត្តប្រព័ន្ធការពារ
៣. ការរកឲ្យឃើញភាពមិនប្រក្រតីផ្សេងៗក្នុងអ៊ិនធើណិតនៅពេលវាកើតមានឡើង
៤. ការឆ្លើយតបនឹងព្រឹត្តិការណ៍អ៊ិនធើណិតផ្សេងៗនៅពេលរកវាឃើញ
៥. ការស្តារមកកាន់ស្ថានភាពដើមវិញ បន្ទាប់ពីកើតមានហេតុការណ៍ក្នុងអ៊ិនធើណិត

ការផ្តល់មតិទី៦៖ របៀបរបបអនុវត្តល្អៗនៅអន្តរជាតិ ក៏គួរយកមកកែសម្រួលប្រើដែរ ដើម្បីធ្វើការវាយតម្លៃជាលក្ខណៈប្រព័ន្ធ និងតាមដានកម្រិតភាពធន់ នៃសន្តិសុខអ៊ិនធើណិតនាបច្ចុប្បន្ន ហើយអាចរកឃើញចន្លោះខ្វះខាតនៅក្នុងវិធានការទប់ស្កាត់ និងសម្រាលគ្រោះថ្នាក់ផ្សេងៗ។ នៅពេលរកឃើញចន្លោះខ្វះខាតទាំងនេះហើយ គួរកំណត់អាទិភាពឲ្យវា ដោយផ្អែកលើទំហំគ្រោះថ្នាក់ទៅដល់ ប្រព័ន្ធហេដ្ឋារចនាសម្ព័ន្ធឌីជីថលកម្ពុជា ក្នុងនោះមានទាំង ការវិភាគពីការគំរាមកំហែង និងលទ្ធភាពមានការវាយប្រហារតាមអ៊ិនធើណិតផង។ នៅពេលកំណត់កម្រិតនៃហានិភ័យនិងការគំរាមកំហែងបានហើយ គួរមានលើកសំណើពីដំណោះស្រាយទៅដល់ថ្នាក់ដឹកនាំជាន់ខ្ពស់ ដើម្បីសុំការឧបត្ថម្ភគាំទ្រ និងមូលនិធិ។

ការផ្តល់មតិទី៧៖ សន្តិសុខអ៊ិនធើណិតជាប្រធានបទមួយដែលគ្រប់គ្នាត្រូវយល់ដឹង ហើយសហគមន៍ព័ត៌មានវិទ្យា (IT) គួរជួយធ្វើឲ្យព័ត៌មានមានលក្ខណៈសាមញ្ញងាយយល់ និងគួរកាត់បន្ថយការប្រើពាក្យបច្ចេកទេស និងពាក្យពេចន៍មានប្រើតែក្នុងជំនាញរបស់ខ្លួន ដែលអាចរារាំងដល់ការប្រាស្រ័យទាក់ទងគ្នាបានច្បាស់លាស់ល្អ និងការបំផុសចំណាប់អារម្មណ៍។

ការផ្តល់មតិទី៨៖ ដើម្បីសម្រេចតាមគោលដៅភាពធន់នៃប្រព័ន្ធអ៊ិនធើណិត ការកំណត់តាំងពីដើមទីនូវរង្វាស់ជាក់លាក់ដោយមានការឯកភាពគ្នាពីអ្នកពាក់ព័ន្ធនានា អាចជួយពង្រឹងទំនុកចិត្តនិងការគាំទ្រដល់អ្នកចូលរួមទាំងឡាយ។ ក្នុងនេះអង្គភាពទទួលបន្ទុកលើអភិបាលកិច្ចសន្តិសុខអ៊ិនធើណិត មានភារកិច្ចជំរុញឲ្យ អ្នកពាក់ព័ន្ធនានាអនុវត្តវិធីសាស្ត្រសកម្មឈានមុខដោយអាចប្រើប្រាស់លក្ខខ័ណ្ឌតម្រូវផ្សេងៗ និងបទបញ្ញត្តិស្តីពីសន្តិសុខអ៊ិនធើណិត ដើម្បីសម្រេចគោលដៅរបស់ខ្លួន។

ការផ្តល់មតិទី៩៖ ចំណេះដឹងជំនាញផ្នែកសន្តិសុខអ៊ិនធើណិតអាចកសាងឡើងបានតាមរយៈ សហប្រតិបត្តិការ និងការផ្លាស់ប្តូរបទពិសោធន៍គ្នា។ អាស៊ានបានជឿនលឿនទៅមុខច្រើនក្នុងការបង្កើត គំនិតផ្តួចផ្តើមផ្នែកអភិបាលកិច្ចសន្តិសុខអ៊ិនធើណិតក្នុងតំបន់ដែលកម្ពុជាអាចស្រង់យកមកប្រើប្រាស់បាន។ ជាក់ស្តែងកម្ពុជា គួរពិចារណាចូលរួមឲ្យបានខ្លាំងក្លាក្នុងមជ្ឈមណ្ឌលកសាងសមត្ថភាពសន្តិសុខអ៊ិនធើណិតអាស៊ាន-ជប៉ុន។ គោលដៅមួយរបស់មជ្ឈមណ្ឌលនេះគឺ បណ្តុះបណ្តាលអ្នកជំនាញការផ្នែកសន្តិសុខអ៊ិនធើណិតអាស៊ាន ក្នុងការការពារប្រព័ន្ធអ៊ិនធើណិត ការសិក្សាស្រាវជ្រាវលើកុំព្យូទ័រដែលរងគ្រោះថ្នាក់ និងការវិភាគកម្មវិធីកុំព្យូទ័រដែលបង្កផលអាក្រក់ (computer forensics and malware analysis) (JAIF 2018)។ ជំនាញទាំងនេះជួយដោះស្រាយដោយផ្ទាល់នូវ តម្រូវការផ្នែកបច្ចេកទេសក្នុងក្របខ័ណ្ឌសន្តិសុខអ៊ិនធើណិតរបស់ NIST និងតម្រូវការបណ្តុះបណ្តាលអ្នកវិជ្ជាជីវៈកម្ពុជាខាងផ្នែកសន្តិសុខអ៊ិនធើណិត ដែលមានជំនាញឯកទេសគ្រប់គ្រាន់។ កម្ពុជាក៏អាចប្រើកម្មវិធីបណ្តុះបណ្តាលនេះធ្វើជាគំរូមួយ ដើម្បីបង្កើតវគ្គសិក្សាពីសន្តិសុខអ៊ិនធើណិតរបស់ខ្លួនផ្ទាល់ សម្រាប់ដំណើរការនៅតាមសាកលវិទ្យាល័យ និងសម្រាប់កម្មវិធីអប់រំនិងបណ្តុះបណ្តាលវិជ្ជាជីវៈផ្សេងៗ។

ការផ្តល់មតិទី១០៖ ការចេញលិខិតបញ្ជាក់គុណភាពសន្តិសុខអ៊ិនធើណិត ក៏អាចធ្វើឡើងសម្រាប់បុគ្គល និងអាជីវកម្មដែលមានជាស្រេចនូវ ចំណេះដឹងជំនាញផ្នែកសន្តិសុខអ៊ិនធើណិត និងបានប្រតិបត្តិតាមស្តង់ដាឧស្សាហកម្ម ដែលកំណត់ឡើងដោយរដ្ឋាភិបាល ឬ អង្គភាពកំណត់ស្តង់ដាឯកជននៅក្នុងតំបន់។ ឧស្សាហកម្មជាច្រើន បានប្រើប្រាស់បទបញ្ញត្តិរបស់ខ្លួនផ្ទាល់ដើម្បីធ្វើការបញ្ជាក់គុណភាពនេះ ពីព្រោះអង្គភាពកំណត់ស្តង់ដាទាំងឡាយ អាចសម្របខ្លួនទៅនឹងបច្ចេកវិទ្យាថ្មីៗបានលឿនជាង និងការពារអ្នកប្រើប្រាស់បានល្អជាង បើធៀបទៅនឹងករណីដែលអង្គភាពទាំងនេះ ត្រូវពឹងផ្អែកទាំងស្រុងទៅលើដំណើរការរបស់រដ្ឋាភិបាល។ ឧទាហរណ៍ នៅសហរដ្ឋអាមេរិក ស្តង់ដាសន្តិសុខទិន្នន័យរបស់អាជីវកម្មផ្នែកប័ណ្ណទូទាត់ ត្រូវបានបង្កើតឡើងដោយក្រុមប្រឹក្សាអ្នកជំនាញការនៃផ្នែកអាជីវកម្មនេះ ដែលបានតម្រូវឲ្យក្រុមហ៊ុនប័ណ្ណឥណទាន (ឧ. VISA និង Mastercard) អនុវត្តតាមការត្រួតពិនិត្យសន្តិសុខ ដើម្បីកាត់បន្ថយការក្លែងបន្លំប័ណ្ណឥណទាន។ ការត្រួតពិនិត្យសន្តិសុខបន្ថែមទាំងនេះ មិនមែនគ្រាន់តែក្លាយជា បន្ទុកចំណាយបន្ថែមសម្រាប់អាជីវកម្មនោះទេ ប៉ុន្តែវាក៏ក្លាយជាកម្លាំងជម្រុញអាជីវកម្ម និងជាឧត្តមភាពប្រកួតប្រជែងមួយ តាមការពង្រឹងសន្តិសុខទិន្នន័យ និងការការពារឯកជនភាពរបស់អតិថិជននៃសាមីអាជីវកម្មផងដែរ។

សេចក្តីសន្និដ្ឋាន

ចំនួនអ្នកប្រើអ៊ិនធើណិត និងឧបករណ៍ដែលមានការតភ្ជាប់នឹងប្រព័ន្ធអ៊ិនធើណិតនៅកម្ពុជា កំពុងកើនឡើងយ៉ាងលឿន ហើយអសកម្មភាព ក្នុងការកសាងក្របខ័ណ្ឌសន្តិសុខអភិបាលកិច្ចអ៊ិនធើណិតជាតិ អាចនាំឲ្យប្រជាជន និងសេដ្ឋកិច្ចកម្ពុជាជួបហានិភ័យធ្ងន់ធ្ងរមិនអាចទទួលយកបាន។ កិច្ចប្រឹងប្រែងគួរ

ចាប់ផ្តើមពីថ្នាក់លើ ដោយក្រសួងមន្ទីរ និងអាជីវកម្មសំខាន់ៗ ទាំងអស់ ព្រមទាំងប្រជាពលរដ្ឋ ត្រូវចូលរួមយ៉ាងសកម្មដើម្បី ញ៉ាំងឲ្យមានការសម្របសម្រួលល្អ និងលទ្ធផលប្រកបដោយ ចីរភាព។ ដើម្បីអាចមើលឃើញពី ហានិភ័យនៃការវាយប្រហារ តាមអ៊ិនធើណិតទៅលើហេដ្ឋារចនាចម្ព័ន្ធសំខាន់ៗ រដ្ឋាភិបាល គួរពិចារណាកំណត់ឲ្យមន្ត្រីរបស់ខ្លួន និងម្ចាស់អាជីវកម្មពាក់ព័ន្ធ បានទទួលការបណ្តុះបណ្តាល បង្កើនចំណេះដឹងពីសន្តិសុខ អ៊ិនធើណិត ដើម្បីឲ្យមានការយល់ដឹងជាមូលដ្ឋាន អំពីការ គំរាមកំហែងក្នុងវិស័យរៀងៗខ្លួន មុនពេលមានការដាក់អនុវត្ត បទបញ្ញត្តិ ស្តីពីសន្តិសុខអ៊ិនធើណិត ឬបទបញ្ញត្តិស្តីពីបទល្មើស តាមអ៊ិនធើណិត។

នៅពេលរដ្ឋាភិបាលបានកំណត់ច្បាស់លាស់ហើយ នូវ គោលដៅដែលខ្លួនចង់សម្រេចឲ្យបាន មន្ត្រីរដ្ឋាភិបាលគួររៀបចំ គណៈកម្មាធិការចម្រុះមួយនៃស្ថានប័នរដ្ឋនិងឯកជន ដើម្បីកសាង បទបញ្ញត្តិស្តីពី សន្តិសុខអ៊ិនធើណិតដែលផ្តោតលើការការពារ ហេដ្ឋារចនាសម្ព័ន្ធសំខាន់ៗនៅកម្ពុជា ក៏ដូចជាការទទួលស្គាល់ ឯកជនភាពរបស់ពលរដ្ឋ នៅក្នុងអ៊ិនធើណិត ថាជាសិទ្ធិមនុស្ស មួយផងដែរ។ គោលនយោបាយទាំងនេះ គួរលើកទឹកចិត្ត អាជីវកម្មនានានៅកម្ពុជា ឲ្យសម្លឹងទៅរដ្ឋាភិបាលក្នុងការស្វែងរក ធនធាន ដើម្បីពង្រឹងកម្មវិធីសន្តិសុខអ៊ិនធើណិតរបស់ខ្លួន។ កម្ពុជាបានរៀបចំរួចរាល់ហើយនូវ ក្រុមឆ្លើយតបបន្ទាន់នឹងបញ្ហា ជាប់ទាក់ទងជាមួយនឹងកុំព្យូទ័រ ហើយក្រុមនេះគួរទទួលបាននូវ ធនធានមនុស្ស មូលនិធិ និងការបណ្តុះបណ្តាលបច្ចេកទេស ដ៏ចាំបាច់ៗ ដើម្បីអាចក្លាយជាចំណុចកណ្តាលសម្រាប់ឲ្យ រដ្ឋាភិបាល និងអាជីវកម្មឯកជននានាស្វែងរកព័ត៌មានថ្មីទាន់ពេល និងព័ត៌មានសង្ខេបស្តីពី ការគំរាមកំហែងលើសន្តិសុខ និងភាព ងាយរងគ្រោះនៃប្រព័ន្ធអ៊ិនធើណិត។

ម៉្យាងទៀត រដ្ឋាភិបាលគួរពិចារណាធ្វើការវាយតម្លៃក្របខ័ណ្ឌ សន្តិសុខអ៊ិនធើណិត NIST មួយ ដោយចាប់ផ្តើមពីវិស័យអាច មានផលប៉ះពាល់ខ្លាំងជាងគេ ដូចជា ពាណិជ្ជកម្មអេឡិចត្រូនិក និងរដ្ឋាភិបាលអេឡិចត្រូនិក ជាដើម។ ពលរដ្ឋ និងអាជីវកម្មនានា កំពុងពឹងផ្អែកយ៉ាងលឿនទៅលើសេវាទាំងនេះ សម្រាប់ការធ្វើ ប្រតិបត្តិការធនាគារតាមអ៊ិនធើណិត ប្រតិបត្តិការពីអាជីវកម្ម មួយទៅអាជីវកម្មមួយ ការបង់ថ្លៃទឹកនិងអគ្គិសនីតាមអ៊ិនធើណិត និងសេវាផ្សេងៗទៀត។ ការវាយតម្លៃសន្តិសុខអ៊ិនធើណិតតាម ដំណាក់កាល អាចនាំឲ្យមានការកំណត់បានកាន់តែត្រឹមត្រូវនូវ កាលបរិច្ឆេទសម្រេចគោលដៅ និងសហប្រតិបត្តិកាន់តែច្រើន ទៀតរវាងក្រសួងនានា។

ឯកសារយោង

Council of Councils. 2019. Ranking the Top Global Challenges. Report Card on International Cooperation. www.cfr.org/interactive/councilofcouncils/reportcard2019/#!/ranking/2019.

JAIF (Japan-ASEAN Integration Fund). 2018. “ASEAN-Japan Cybersecurity Capacity Building Centre (Step 2).” https://jaif.asean.org/support/project-brief/asean-japan-cybersecurity-capacity-building-centre.html.

Kepios Analysis. 2019. “Digital in Cambodia.” https://datareportal.com/digital-in-cambodia.

NIST (National Institute of Standards and Technology). 2018. Framework for Improving Critical Infrastructure Cybersecurity. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Ou Phannarith. 2018. “Cybercrime and Legislation in Cambodia.” Paper presented at the AFIN and Cybersecurity Workshop, Phnom Penh, Cambodia, 3 April 2018.

Republic of Singapore. 2018. Cybersecurity Act 2018.

RGC. 2014. Unofficial Draft of Cybercrime Law. https://www.ccimcambodia.org/wp-content/uploads/2014/10/draft_cybercrime_law_en.pdf

Seangly Phak. 2013. “‘Developed’ by 2050: PM.” Phnom Penh Post, 7 Jun 2013. www.phnompenhpost. com/national/%E2%80%98developed%E2%80%99-2050-pm.

World Bank. 2019. “Cambodia Annual GDP Growth.” https://data.worldbank.org/indicator/NY.GDP.M KTP.KD.ZG?%20end=2018&locations=KH&most_recent_value_desc=true&start= 1994&view=chart.