សាកលវិទ្យាល័យភូមិន្ទនីតិសាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច

Université Royale de Droit et des sciences Economiques

Royal University of Law and Economics

សារណាបញ្ចប់ការសិក្សា

បទល្មើសព័ត៌មានវិទ្យានៅកម្ពុជា

ស្រាវជ្រាវចាប់ពីថ្ងៃទី២៧ ខែមេសា ឆ្នាំ២០២១ ដល់ថ្ងៃទី ២៥ ខែមិថុនា ឆ្នាំ២០២១

តាក់តែងឡើងដោយ

និស្សិតឈ្មោះ **ប៉ែន សៀងមៀ**

សាស្ត្រាចារ្យណែនាំ

សាស្ត្រាចារ្យ ហោ សុភ័ណ្ឌ

ថ្នាក់បរិញ្ញាបត្រ **នីតិសាស្ត្រ**

ជំនាន់ទី ២១

ឆ្នាំចូលសិក្សា ២០១៧

ឆ្នាំសរសេរសារណា ២០២១

សេចក្តីថ្លែងអំណរគុណ

ខ្ញុំបាទឈ្មោះ **ម៉ែន សៀងហៅ** ជានិស្សិតថ្នាក់បរិញ្ញាបត្រនីតិសាស្ត្រ ឆ្នាំទី៤ ជំនាន់ទី២១ នៃសាកលវិទ្យាល័យភូមិន្ទនីតិសាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច ឆ្នាំសិក្សា២០២០-២០២១ សូមថ្លែងអំណរគុណ ជូនចំពោះ៖

- លោកឪពុក **ហាស សាម៉ែត** និងអ្នកម្តាយ **សេន សុភា** ដែលបានផ្តល់កំណើត បីបាច់ថែរក្សាអប់រំ ទូន្មានប្រៀនប្រដៅប្រកបដោយព្រហ្មវិហារធម៌ទាំង ៤ (បួន) ចំពោះកូន តាំងពីតូចរហូតមកដល់ពេលបច្ចុប្បន្ន ។ ក៏ព្រោះតែទឹកដោះម្តាយថ្លៃទើបកូនមានថ្ងៃនេះ ។ លោកដ៏មានគុណទាំងទ្វេបានលះបង់គ្រប់បែបយ៉ាង ជម្នះរាល់គ្រប់ឧបសគ្គ និងខិតខំប្រឹងប្រែងតស៊ូយ៉ាងលំបាកតែមិនរាថយ ដើម្បីស្វែងរកនូវធនធានសម្រាប់ផ្គត់ផ្គង់ការរៀនសូត្ររបស់កូន ។ ជាងនេះទៀត លោកដ៏មានគុណទាំងពីរ បានដើរតួយ៉ាងសំខាន់ ក្នុងការជម្រុញលើកទឹកចិត្ត បណ្តុះបណ្តាលកូន ដើម្បីក្លាយជាកូនល្អ សិស្សល្អ និងពលរដ្ឋល្អ ក្នុងសង្គមជាតិ ។
- ឯកឧត្តមបណ្ឌិត **ឈុយ ចន្ធឿ** សាកលវិទ្យាធិការ នៃសាកលវិទ្យាល័យភូមិន្ទនីតិសាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច និងសាកលវិទ្យាធិការរង ថ្នាក់ដឹកនាំគ្រប់ជាន់ថ្នាក់ ព្រមទាំងលោក លោកស្រីសាស្ត្រាចារ្យនៃសាកលវិទ្យាល័យភូមិន្ទនីតិសាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ចទាំងអស់ ដែលបានលះបង់ពេលវេលាដ៏មានតម្លៃ ក្នុងការបង្ហាត់បង្រៀន និងចែករំលែកបទពិសោធន៍ ប្រកបដោយក្រមសីលធម៌ និងមានវិជ្ជាជីវៈពិតប្រាកដ ដល់រូបខ្ញុំ ក្នុងរយៈកាលប្រមាណ ៤ (បួន) ឆ្នាំ កន្លងមកនេះ ។
- លោកសាស្ត្រាចារ្យ **ហោ សុគ័ណ្ឌ** ប្រធានការិយាល័យសិក្សា នៃសាកលវិទ្យាល័យភូមិន្ទនីតិសាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច ដែលជាសាស្ត្រាចារ្យដឹកនាំការស្រាវជ្រាវចំពោះប្រធានបទសារណាបញ្ចប់ការសិក្សាមួយនេះ ។ លោកសាស្ត្រាចារ្យ បានព្យាយាមចំណាយពេលវេលាដ៏មានតម្លៃ និងបានបណ្តុះបណ្តាល បង្ហាត់បង្ហាញ ខ្ញុំបាទឱ្យចងក្រងនូវស្នាដៃមួយនេះ ប្រកបទៅដោយការយកចិត្តទុកដាក់បំផុត ដើម្បីឱ្យសារណាបញ្ចប់ការសិក្សាទាំងមូលមានអត្ថន័យ អត្ថរស និងខ្លឹមសារប្រកបទៅដោយលក្ខណៈប្រសើរឡើង ។
- រៀមច្បង និងមិត្តនិស្សិតរួមជំនាន់ទាំងអស់ ដែលបានជ្រោមជ្រែងយ៉ាងសកម្មក្នុងការផ្តល់នូវកម្លាំងចិត្ត និងបានចែករំលែកនូវចំណេះដឹង ព្រមទាំងបំផុសគំនិតល្អៗ ដើម្បីជម្រុញឱ្យសារណាបញ្ចប់ការសិក្សាមួយនេះ មានអត្ថន័យកាន់តែស៊ីជម្រៅ និងក្បោះក្បាយ ។

ជាចុងក្រោយនេះ ខ្ញុំបាទ សូមលំឱនកាយគោរពបួងសួងជូនចំពោះ អ្នកមានគុណទាំងទ្វេ ព្រមទាំង ឯកឧត្តម លោកជំទាវ លោក លោកស្រី អ្នកនាង កញ្ញា សូមឱ្យជួបនូវពុទ្ធពរទាំង៤(បួន)ប្រការ គឺ អាយុ វណ្ណៈ សុខៈ ពលៈ កុំបីឃ្លៀងឃ្លាត ឡើយ ។

អារម្ភកថា

ដោយមើលឃើញថា បទល្មើសព័ត៌មានវិទ្យានៅកម្ពុជា គឺជាបញ្ហាមួយក្នុងចំណោមបញ្ហាជាច្រើនទៀត ដែលកំពុងតែកើតមាននៅកម្ពុជា ដែលបង្កនូវព្យសនកម្មជាច្រើនដូចជាវិស័យសេដ្ឋកិច្ច ពាណិជ្ជកម្ម ជាពិសេស គឺព្យសនកម្មដល់អ្នកប្រើប្រាស់អ៊ីនធឺណិត ។ ក្នុងនាមយើងជាកោសិកាមួយនៃសង្គមកម្ពុជាគួរគប្បីមានការ ព្រួយបារម្ភ និងឈ្វេងយល់ ព្រមទាំងគប្បីដឹងអំពីយុទ្ធសាស្ត្រការពារខ្លួនពីការវាយប្រហាររបស់ចោរបច្ចេកវិទ្យា ។ ស្របពេលជាមួយគ្នានេះ រាជរដ្ឋាភិបាលនីតិកាលទី៦ នៃរដ្ឋសភាដែលដឹកនាំដោយ **សម្តេចអគ្គមហា សេនាបតីតេជោ ហ៊ុន សែន** នាយករដ្ឋមន្ត្រី នៃព្រះរាជាណាចក្រកម្ពុជា បានដាក់ចេញនូវយុទ្ធសាស្ត្រ ចតុកោណដំណាក់កាលទី៤ ដោយធ្វើវិភាជន៍ធនធានបន្ថែមដល់វិស័យសុខាភិបាល អប់រំ សង្គមកិច្ច ជាពិសេសគឺបច្ចេកវិទ្យា ។

ការរីកចម្រើនផ្នែកបច្ចេកវិទ្យា បានជម្រុញដល់ការរីកលូតលាស់ ការងារ នយោបាយ សេដ្ឋកិច្ច និងសង្គម កិច្ច ដែលធ្វើឱ្យកម្ពុជាមានទំនាក់ទំនងជាមួយបណ្តាប្រទេសក្នុងតំបន់ និងពិភពលោក ។ ការរីកចម្រើនផ្នែក ព័ត៌មានវិទ្យា មិនសុទ្ធតែមានផលវិជ្ជមានទាំងស្រុងនោះទេ បើទោះបីជាភាពចាំបាច់នៃបច្ចេកវិទ្យានេះក៏ដោយក្តី ការរីកចម្រើននៃបច្ចេកវិទ្យា គឺជាអាវុធមុខពីរ ពោលគឺមានទាំងផលវិជ្ជមាន និងផលអវិជ្ជមាន ។

ស្របពេលជាមួយគ្នានេះដែល ខ្ញុំបាទដែលជានិស្សិតថ្នាក់បរិញ្ញាបត្រឆ្នាំទី ៤ នៃសាកលវិទ្យាល័យភូមិន្ទ នីតិសាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច បានសិក្សាស្រាវជ្រាវ និងចងក្រងអត្ថបទសារណាស្តីពី "**បទល្មើស ព័ត៌មានវិទ្យានៅកម្ពុជា**" ក្រោមការដឹកនាំដ៏ថ្លៃថ្លារបស់លោក **ហោ សុភ័ណ្ឌ** សាស្ត្រាចារ្យ និងជាប្រធាន ការិយាល័យសិក្សា មហាវិទ្យាល័យនីតិសាស្ត្រ នៃសាកលវិទ្យាល័យភូមិន្ទនីតិសាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច ។ ដោយហេតុថា ខ្ញុំបាទបានកត់សម្គាល់ឃើញថា អត្ថិភាពនៃក្របខណ្ឌច្បាប់នៅមានភាពចន្លោះប្រហោង ប្រជាពលរដ្ឋមួយចំនួនមិនទាន់បានយល់ដឹងអំពីសុវត្ថិភាពនៃការប្រើប្រាស់បច្ចេកវិទ្យា និងកំពុងតែទទួល រងនូវព្យសនកម្មពីបទល្មើសព័ត៌មានវិទ្យា ជាពិសេសប្រធានបទនេះមិនសូវមានអ្នកសរសេរ ។ លើសពីនេះខ្ញុំ បាទ បានខិតខំស្រាវជ្រាវទាំងច្បាប់ជាតិ និងអន្តរជាតិ ព្រមទាំងឯកសារសំខាន់ផ្សេងៗទៀត ដើម្បីចងក្រង និង រៀបចំអត្ថបទសារណានេះឡើង ដោយរំពឹងយ៉ាងមុតមាំថា នឹងទទួលបានសមទ្ធិផលដ៏ប្រសើរ ។

ជាកិច្ចបញ្ចប់ ខ្ញុំបាទទន្ទឹងរង់ចាំនូវរាល់មតិទាំងឡាយក្នុងគោលបំណងស្ថាបនា ពីសំណាក់ឯកឧត្តម លោកជំទាវ លោក លោកស្រី អ្នកនាង កញ្ញា សាស្ត្រាចារ្យ សិស្ស និស្សិត និងមិត្តអ្នកអានទាំងអស់ដើម្បីជាការ កែលម្អដល់រូបខ្ញុំបាទ ។ ដោយក្តីគោរពរាប់អានពីរូបខ្ញុំបាទ ។

មាតិកា

ទំព័រ

បញ្ជីវាក្យសព្ទ iii

សេចក្តីផ្តើម **១**

ជំពូកទី ១

សញ្ញាណទូទៅនៃបទល្មើសព័ត៌មានវិទ្យានៅកម្ពុជា

ផ្នែកទី ១ ៖ សាវតា និងមូលហេតុនៃការកើតមានបទល្មើសព័ត៌មានវិទ្យា **៣**

កថាខណ្ឌទី ១ ៖ សាវតានៃបទល្មើសព័ត៌មានវិទ្យា **៣**

កថាខណ្ឌទី ២ ៖ មូលហេតុនៃការកើតមានបទល្មើសព័ត៌មានវិទ្យា **៥**

ផ្នែកទី ២ ៖ ក្របខណ្ឌច្បាប់ និងសេចក្តីព្រាងច្បាប់ **៧**

កថាខណ្ឌទី ១ ៖ ក្របខណ្ឌច្បាប់ **៧**

កថាខណ្ឌទី ២ ៖ សេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន **៧**

ជំពូកទី ២

បទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យា និងស្ថាប័នជំនាញ

ផ្នែកទី ១ ៖ បទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យា **១២**

កថាខណ្ឌទី ១ ៖ បទចូលទៅដល់ ឬ ស្ថិតនៅនឹងប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យ **១៣**

កថាខណ្ឌទី ២ ៖ បទបង្កើតជាឧបសគ្គដល់ដំណើរការនៃប្រព័ន្ធប្រព្រឹត្តកម្មស្វ័យប្រវត្តនៃទិន្នន័យ **១៥**

កថាខណ្ឌទី ៣ ៖ បទបញ្ចូល លុបបំបាត់ ឬ កែប្រែដោយទុច្ចរិតនូវទិន្នន័យ **១៦**

កថាខណ្ឌទី ៤ ៖ បទចូលរួមក្នុងក្រុមប្រមូលផ្តុំ ឬ បទចូលរួមក្នុងក្រុមប្រមូលផ្តុំ ឬ ក្នុងសន្ធិដ្ឋិភាពដើម្បីរៀបចំប្រព្រឹត្តបទល្មើស **១៨**

កថាខណ្ឌទី ៥ ៖ ការប៉ុនប៉ង **១៩**

កថាខណ្ឌទី ៦ ៖ ទោសបន្ថែម **១៩**

ផ្នែកទី ២ ៖ ស្ថាប័នជំនាញ **២០**

កថាខណ្ឌទី ១ ៖ នាយកដ្ឋានប្រឆាំងនឹងបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន **២១**

កថាខណ្ឌទី ២ ៖ ការិយាល័យឆ្លើយតបបញ្ហាបន្ទាន់នៃកុំព្យូទ័រ **២៣**

ជំពូកទី ៣

យុទ្ធសាស្ត្រឈ្នះឈ្នះប្រឆាំងនឹងបទល្មើសព័ត៌មានវិទ្យា

ផ្នែកទី ១ ៖ យុទ្ធសាស្ត្រឈ្នះឈ្នះសម្រាប់អ្នកប្រើប្រាស់កុំព្យូទ័រ និងទូរស័ព្ទ **២៥**

កថាខណ្ឌទី ១ ៖ កុំព្យូទ័រ(Computor) **២៦**

កថាខណ្ឌទី ២ ៖ ទូរស័ព្ទវៃឆ្លាត(Smart Phone) **២៦**

ផ្នែកទី ២ ៖ យុទ្ធសាស្ត្រឈ្នះឈ្នះសម្រាប់អ្នកប្រើប្រាស់បណ្តាញសង្គម **២៨**

កថាខណ្ឌទី ១ ៖ ហ្វេសប៊ុក(Facebook) **២៩**

កថាខណ្ឌទី ២ ៖ តេលេក្រាម(Telegram) **៣១**

សេចក្តីសន្និដ្ឋាន **៣៦**

អនុសាសន៍ **៣៨**

ឯកសារយោង

បញ្ជីឧបសម្ព័ន្ធ

បញ្ជីនាមសព្ទ

- **អ៊ីនធឺណិត៖** សំដៅដល់បណ្តាញកុំព្យូទ័រពិភពលោកដែលអាចឱ្យមនុស្សចែករំលែកព័ត៌មាន និងទាក់ទងគ្នាទៅវិញទៅមក ។
- **អេឡិចត្រូនិក៖** សំដៅដល់អ្វីដែលពាក់ព័ន្ធនឹងបច្ចេកវិទ្យាដែលមានចរន្តអគ្គិសនី ឌីជីថល ម៉ាញេទិច អុបទិក ឬ បច្ចេកវិទ្យាដែលមានមុខងារប្រហាក់ប្រហែលផ្សេងទៀត ។
- **ប្រព័ន្ធទិន្នន័យ៖** ប្រព័ន្ធមួយដែលមានទិន្នន័យ ទម្រង់ទិន្នន័យ និងប្រព័ន្ធគ្រប់គ្រងទិន្នន័យ ។
- **ឧស្សាហកម្ម៤.0៖** បរិបទនៃការវិវឌ្ឍឧស្សាហកម្មដែលបច្ចេកវិទ្យាអនុញ្ញាតឱ្យមានការបញ្ចូលគ្នា នៃទិន្នន័យពីម៉ាស៊ីន ឧបករណ៍ និងសេនស័រ ពីខ្សែច្រវាក់ផលិតកម្ម និងពីការប្រើប្រាស់របស់មនុស្ស ហើយដែលផ្តល់ព័ត៌មានច្បាស់លាស់ និងទាន់ពេលដល់អ្នកផលិត និងអ្នកពាក់ព័ន្ធ សំដៅធ្វើឱ្យប្រសើរឡើងនូវខ្សែច្រវាក់ផលិតកម្មទាំងមូល ។
- **ប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យ៖** សំដៅដល់កម្មវិធីកុំព្យូទ័រ ប្រព័ន្ធកុំព្យូទ័រ ប្រព័ន្ធ ឬ បណ្តាញ អេឡិចត្រូនិក ឬ មធ្យោបាយអេឡិចត្រូនិកផ្សេងទៀតដែលត្រូវបានប្រើប្រាស់សម្រាប់ផ្ញើដំណឹង ឬ ឆ្លើយតប ។

សេចក្តីផ្តើម

បទល្មើសព័ត៌មានវិទ្យា ចារីងាយស្រួលប្រព្រឹត្តណាស់ ជាទូទៅឱ្យតែមានកុំព្យូទ័រ ដែលភ្ជាប់អ៊ីនធឺណិត ចារីអាចប្រព្រឹត្តបទល្មើសបានហើយ រីឯព្យសនកម្មនៃបទល្មើសនេះក៏មានវិសាលភាពធំសម្បើម ។[1] រហូតដល់ **សម្តេចអគ្គមហាសេនាបតីតេជោ ហ៊ុន សែន** នាយករដ្ឋមន្ត្រី នៃព្រះរាជាណាចក្រកម្ពុជាបានថ្លែងសន្ទរកថា "យើងតម្រូវឱ្យមានច្បាប់បី ឱ្យទៅជាមួយគ្នា គឺច្បាប់ស្តីពី របបសារព័ត៌មានឆ្នាំ១៩៩៥ ច្បាប់ស្តីពីសិទ្ធិទទួលបានព័ត៌មាន(ដែលនៅជាសេចក្តីព្រាងច្បាប់) និងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន(ដែលនៅជាសេចក្តីព្រាងច្បាប់) ច្បាប់ទាំងបីនេះត្រូវតែមានសង្គតិភាព និងបំពេញឱ្យគ្នាទៅវិញទៅមក ។ សម្តេចថ្លែងបន្តទៀតថា ក្នុងពេលជាមួយគ្នានេះ នៅក្នុងសម័យប្រជុំពេញអង្គ បណ្តាប្រទេសបែកអឺរ៉ុបបានឡើងថ្លែងសន្ទរកថា ព្រមទាំងពេលទទួលទានអាហារ ថាគ្មានប្រទេសមួយណាភ្លេចអំពីព្រឹត្តិការណ៍បទល្មើសបច្ចេកវិទ្យាព័ត៌មានឡើយ ដូច្នេះសូម្បីតែប្រទេសដែលគោរពសិទ្ធិបញ្ចេញមតិហើយនោះ ក៏បង្កើតនូវការព្រួយបារម្ភ អំពីបញ្ហាទាក់ទងទៅនឹងបច្ចេកវិទ្យាព័ត៌មាន រហូតដល់ប្រទេសខ្លះនៅអឺរ៉ុប ដែលគេចាត់ទុកថាជាប្រទេសបិតាប្រជាធិបតេយ្យ ក៏ត្រូវបានបង្កើតច្បាប់រារាំង និងទប់ស្កាត់ ដើម្បីដាក់ទណ្ឌកម្មទៅលើការរំលោភបំពានដែលកើតឡើងពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន នេះផងដែរ ។[2]

គួសបញ្ជាក់ថា នៅក្នុងឆ្នាំ២០១២ រដ្ឋាភិបាលនៃប្រទេសកម្ពុជាបានធ្វើការជូនដំណឹងថា កម្ពុជាកំពុងតែព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន ដើម្បីឆ្លើយតបបញ្ហាទៅនឹងតថភាពសង្គមជាក់ស្តែង ។[3] រហូតមកដល់បច្ចុប្បន្ននេះ កម្ពុជាយើងក៏មិនទាន់មានច្បាប់នេះនៅឡើយ ពោលរដ្ឋាភិបាលដែលមានក្រសួងមហាផ្ទៃជាសេនាធិការ មានសមត្ថកិច្ចក្នុងការព្រាងច្បាប់នេះ ។[4] បើទោះបីជាកម្ពុជាពុំទាន់មានច្បាប់ពិសេសស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន ក៏កម្ពុជាមានបទដ្ឋានគតិយុត្តិសមល្មមនឹងដាក់ទោសទណ្ឌលើជនល្មើសដែលប្រព្រឹត្តបទល្មើសព័ត៌មានវិទ្យាដែរ ពោលបច្ចុប្បន្ននេះកម្ពុជាកំពុងប្រើក្រមព្រហ្មទណ្ឌ ឆ្នាំ២០០៩ ដែលកំពុងនៅជាធរមាន ។

មានចម្ងល់មួយចំនួនចោទសួរឡើងថាតើ សញ្ញាណទូទៅនៃបទល្មើសព័ត៌មានវិទ្យានៅកម្ពុជាសិក្សាទៅលើអ្វីខ្លះ? និងស្ថាប័នជំនាញណាខ្លះដែលមានភារកិច្ចចម្បងក្នុងការបង្ការ បង្ក្រាប ឆ្លើយតប និងស្រាវជ្រាវស៊ើប

[1] https://searchsecurity.techtarget.com/definition/cybercrime (ចូលទស្សនានៅថ្ងៃទី ១០ ខែមិថុនា ឆ្នាំ២០២១)។

[2] Fresh News.com (ចូលទស្សនានៅថ្ងៃទី ១០ ខែមិថុនា ឆ្នាំ២០២១)។

[3] Freedom House, សិទ្ធិសេរីភាពនៅលើប្រព័ន្ធអ៊ីនធឺណិត, (២០១៣), ទំព័រទី៨, អាចរកបាននៅ Cambodia Final 2013 (freedomhouse.org)។

[4] https://www.interior.gov.kh/news/detail/2002 (ចូលទស្សនានៅថ្ងៃទី២០ ខែមិថុនា ឆ្នាំ២០២១)។

អង្កេតចំពោះបទល្មើសព័ត៌មានវិទ្យា? និងថាតើមានយុទ្ធសាស្ត្រឈ្នះឈ្នះអ្វីខ្លះ ដើម្បីប្រឆាំងទៅនឹងបទល្មើសព័ត៌មានវិទ្យានៅកម្ពុជា?

ប្រធានបទ "**បទល្មើសព័ត៌មានវិទ្យានៅកម្ពុជា**" នេះ មានគោលបំណងបង្ហាបការយល់ដឹងបន្ថែមដល់បុគ្គលដែលអនុវត្តច្បាប់ដូចជាមន្ត្រីនគរបាលយុត្តិធម៌ ចៅក្រម ព្រះរាជអាជ្ញា មេធាវី ជាអាទិ៍ ។ ជាងនេះទៅទៀត ប្រធានបទនេះ ក៏មានគោលបំណងផ្តល់ជាគតិដល់អ្នកប្រើប្រាស់បណ្តាញសង្គម អ្នកប្រើប្រាស់ប្រព័ន្ធបច្ចេកវិទ្យា ដើម្បីឱ្យបុគ្គលទាំងនេះយល់ដឹងអំពីយុទ្ធសាស្ត្រការពារខ្លួនជៀសវាងពីការវាយប្រហាររបស់ចោរបច្ចេកវិទ្យា ។

ដើម្បីជាជំហានឈានទៅដល់ការបកស្រាយប្រធានបទនេះឱ្យកាន់តែងាយស្រួល និងយល់ច្បាស់ជាងនេះទៅទៀតនោះ យើងសូមធ្វើការបែងចែកប្រធានបទនេះជា៣(បី)ជំពូក រួមមាន **សញ្ញាណទូទៅនៃបទល្មើសព័ត៌មានវិទ្យានៅកម្ពុជា**(ជំពូកទី១) **បទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យានិងស្ថាប័នជំនាញ**(ជំពូកទី២) និង **យុទ្ធសាស្ត្រឈ្នះឈ្នះប្រឆាំងនឹងបទល្មើសព័ត៌មានវិទ្យានៅកម្ពុជា**(ជំពូកទី៣) ។

ជំពូកទី១
សញ្ញាណទូទៅនៃបទល្មើសព័ត៌មានវិទ្យានៅកម្ពុជា

ប្រធានបទខាងលើយើងឃើញថា មានវាក្យស័ព្ទមួយគឺ បទល្មើសព័ត៌មានវិទ្យា ។ គួសបញ្ជាក់ថា បទល្មើសព័ត៌មានវិទ្យា ឬ បទល្មើសបច្ចេកវិទ្យាព័ត៌មាន យើងអាចប្រើវាក្យស័ព្ទមួយណាក៏បានដែរ ។ បទល្មើសព័ត៌មានវិទ្យា មានចែងនៅក្នុងក្រមព្រហ្មទណ្ឌ ក៏ប៉ុន្តែមិនបានចែងអំពីនិយមន័យនោះទេ ។

បទល្មើសព័ត៌មានវិទ្យា គឺជាបទល្មើសដែលប្រព្រឹត្តនៅក្នុងបណ្តាញបច្ចេកវិទ្យាគមនាគមន៍ និងព័ត៌មាន ដូចជា ការចូលលួច ក្លែងបន្លំ ឬ កែឯកសារ ការបញ្ចូលមេរោគ ការផ្ញើសារគំរាមកំហែង ឬ ចាប់ជំរិត ឬ ការធ្វើឱ្យប៉ះពាល់ដល់សន្តិសុខសេដ្ឋកិច្ច និងសង្គមកិច្ច ។[5] មានន័យថា បទល្មើសព័ត៌មានវិទ្យាជាបទល្មើសសកលដែលកើតឡើងមាននៅទូទាំងពិភពលោក ដោយសារនៅលើពិភពលោក ប្រទេសណាក៏ដោយក៏ប្រើប្រាស់អ៊ីនធឺណិត បើគិតពីធាតុសត្យាម័តនៃបទល្មើស គឺជនល្មើសប្រើប្រាស់ឧបករណ៍បច្ចេកវិទ្យាដូចជា កុំព្យូទ័រ ប្រព័ន្ធកុំព្យូទ័រ ប្រព័ន្ធអ៊ីនធឺណិត កម្មវិធីបណ្តាញសង្គម ការប៉ុនប៉ងប្រើប្រាស់មធ្យោបាយបច្ចេកវិទ្យាក្នុងគោលបំណងបំផ្លិចបំផ្លាញប្រព័ន្ធកុំព្យូទ័រ ប្រព័ន្ធបណ្តាញកុំព្យូទ័រ ការកែប្រែនូវទិន្នន័យ ឬក៏លួចទិន្នន័យកុំព្យូទ័រ ការចែកចាយរូបភាពអាសអាភាសកុមារ ដើម្បីធ្វើជាមធ្យោបាយប្រព្រឹត្តបទល្មើស ។

យើងដឹងតែនិយមន័យប៉ុណ្ណោះមិនទាន់អាចយល់ប្រធានបទទាំងស្រុងនោះ ដើម្បីយល់កាន់តែច្បាស់អំពីសញ្ញាណទូទៅនៃបទល្មើសព័ត៌មានវិទ្យាជាងនេះទៀត យើងគួរគប្បីសិក្សាអំពី **សាវតានិងមូលហេតុនៃការកើតមានបទល្មើសព័ត៌មានវិទ្យានៅកម្ពុជា**(ផ្នែកទី១) និង**ក្របខណ្ឌច្បាប់និងសេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន**(ផ្នែកទី២) ។

ផ្នែកទី ១ សាវតា និងមូលហេតុនៃការកើតមានបទល្មើសព័ត៌មានវិទ្យានៅកម្ពុជា

សូមបញ្ជាក់ថា ក្រោយពីសង្គ្រាមឆ្នាំ១៩៧៩បានបញ្ចប់ កម្ពុជាបានខិតខំប្រឹងប្រែងអភិវឌ្ឍខ្លួនរហូតដល់ក្លាយជាប្រទេសកំពុងអភិវឌ្ឍន៍នាពេលបច្ចុប្បន្ន ។ ស្របពេលនៃការរីកចម្រើន បច្ចេកវិទ្យាក៏បានរីកចម្រើនគួរកត់សម្គាល់ ហើយបទល្មើសព័ត៌មានក៏រឹងរឹតតែកើតមានមិនតិចទេ ។[6] ការកើតមានបទល្មើសនីមួយៗតែងមានមូលហេតុ ។ នៅក្នុងផ្នែកនេះយើងនិងសិក្សាអំពី **សាវតានៃបទល្មើសព័ត៌មានវិទ្យានៅកម្ពុជា**(កថាខណ្ឌទី១) និង**មូលហេតុនៃការកើតមានបទល្មើសព័ត៌មានវិទ្យានៅកម្ពុជា**(កថាខណ្ឌទី២) ។

កថាខណ្ឌទី ១ សាវតានៃបទល្មើសព័ត៌មានវិទ្យានៅកម្ពុជា

នៅឆ្នាំ១៩៩៧ កម្ពុជាចាប់ផ្តើមមានប្រព័ន្ធអ៊ីនធឺណិតប្រើប្រាស់ជាលើកដំបូង និងមានតែពីរបណ្តាញ

[5]ឧត្តមក្រុមប្រឹក្សាសេដ្ឋកិច្ចជាតិ, ក្របខណ្ឌគោលនយោបាយសេដ្ឋកិច្ច និងសង្គមឌីជីថលកម្ពុជា, (១០ ឧសភា ២០២១), លេខ ១២, ទំព័រ៩៨។

[6]https://www.interior.gov.kh/news/detail/2002 (ចូលទស្សនានៅថ្ងៃទី ២០ ខែឧសភា ឆ្នាំ២០២១)។

ទេគឺ ក្រុមហ៊ុនរដ្ឋ **Camnet** និងក្រុមហ៊ុន **Bigpond Telstra** របស់ប្រទេសអូស្ត្រាលី តាមប្រព័ន្ធផ្កាយរណប ក្នុងល្បឿន **64Kbps**។[7] ចាប់តាំងពីឆ្នាំ២០០២ គេហទំព័ររាជរដ្ឋាភិបាលកម្ពុជាមួយចំនួនដូចជា ក្រសួងការបរទេស គណៈកម្មការជាតិរៀបចំការបោះឆ្នោត នគរបាលជាតិ តុលាការកំពូល និងក្រសួងការពារជាតិ បានក្លាយជាមុខព្រួញនៃការវាយប្រហារតាមអ៊ីនធឺណិត ។ នៅក្នុងឆ្នាំ២០១២ ក្រសួងមហាផ្ទៃបានប្រកាសជាលើកដំបូងអំពីសេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មានដែលមាន**៨(ប្រាំបី)ជំពូក និង៤០(សែសិប) មាត្រា** និងធ្វើការប្រជុំរាប់សិបលើកព្រមទាំងមានជំនួយឧបត្ថម្ភបច្ចេកទេសពីក្រសួងយុត្តិធម៌នៃសហរដ្ឋ-អាមេរិកផងដែរ ។[8] ក្រោយចេញសេចក្តីប្រកាសនេះភ្លាមមានក្រុម **Hacker** មួយឈ្មោះថា **Nullcrew** បានបើកយុទ្ធនាការមួយដែលមានឈ្មោះជាភាសាអង់គ្លេសថា **Operation the pirate bay** ដើម្បីធ្វើការវាយប្រហារគេហទំព័រមួយចំនួនរបស់កម្ពុជាទុកជាការតវ៉ាប្រឆាំងនឹងការរៀបចំការធ្វើសេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន ។ ស្របពេលនោះដែលក៏មានការចាប់ និងបញ្ជូនខ្លួនសហស្ថាបនិកនៃគេហទំព័រ **BitTorrent** នៃក្រុមដែលបើកយុទ្ធនាការ **The pirate bay** គឺ **លោក Gottfrid Svartholm Warg** ដែលមានអាយុ២៧(ម្ភៃប្រាំពីរ)ឆ្នាំ នៅលើទឹកដីកម្ពុជាទៅកាន់ប្រទេសស៊ុយអែត ។[9] នៅក្នុងឆ្នាំដដែល កម្ពុជាបានក្លាយជាប្រធានប្តូរវេនអាស៊ាន ពេល នោះមានក្រុមHacker បានលួចយកឯកសាររបស់ក្រសួងការបរទេសកម្ពុជាជាង ៥០០០(ប្រាំពាន់) ច្បាប់ ។[10] មុនការបោះឆ្នោតឆ្នាំ ២០១៨ ក្រុមហ៊ុនឯកជនមួយនៅសហរដ្ឋអាមេរិកដែលនាំមុខគេក្នុងការងារតាមដានសុវត្ថិភាពលើប្រព័ន្ធអ៊ីនធឺណិតឈ្មោះ **FireEye** រកឃើញថាក្រុម **Hacker** ដ៏ល្បីមួយឈ្មោះថា **TEMP** ដែលមានទំនាក់ទំនងគួរឲ្យសង្ស័យជាមួយនឹងរដ្ឋាភិបាលចិនបានប្រើបច្ចេកវិទ្យាលុកលុយស្ថាប័នជាច្រើនរបស់កម្ពុជា ដែលធ្វើការងារពាក់ព័ន្ធដំណើរការបោះឆ្នោត ។[11] គោលដៅដែលក្រុមចោរបច្ចេកវិទ្យាវាយប្រហារនោះ រួមមានស្ថាប័ន រដ្ឋាភិបាល បក្សប្រឆាំង មន្ត្រីការពារសិទ្ធិមនុស្ស និងអ្នកសារព័ត៌មាន ។ បញ្ហាទាំងនេះបញ្ជាក់ថា បទល្មើសព័ត៌មានវិទ្យាបានវាយប្រហារសុវត្ថិភាពកម្ពុជាគួរឱ្យព្រួយបារម្ភជាខ្លាំង នៅក្នុងខណៈដែលក្របខណ្ឌច្បាប់កម្ពុជាដែលត្រូវយកមកអនុវត្តប្រឆាំងនឹងបទល្មើសទាំងនោះមានភាពមិនច្បាស់លាស់ និងស្រពេចស្រពិល ទន្ទឹមនឹងកម្ពុជាត្រូវបានវាយតម្លៃដោយ

[7] Cambodia ICT Blog (ចូលទស្សនានៅថ្ងៃទី ១៣ ខែមិថុនា ឆ្នាំ២០២១)។

[8] https://www.information.gov.kh/articles/14898 (ចូលទស្សនានៅថ្ងៃទី ១៣ ខែមិថុនា ឆ្នាំ២០២១)។

[9] ងួន សុម៉ាលី និងស្រ៊ុន សុភ័ក្ត្រ ,Cambodia V Hacker: តុល្យភាពរវាយសន្តិសុខ និងសេរីភាព នៅក្នុងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន, ៧៨។

[10] Cybersecurity.com (ចូលទស្សនានៅថ្ងៃទី ១៣ ខែមិថុនា ឆ្នាំ២០២១)។

[11] Financial Times (ចូលទស្សនានៅថ្ងៃទី ១៤ ខែមិថុនា ឆ្នាំ២០២១)។

សហភាពទូរគមនាគមន៍អន្តរជាតិនៅឆ្នាំ២០១៤ ថានៅមានកង្វះការយល់ដឹងបច្ចេកវិទ្យាស៊ីជម្រៅ ដោយសារតែកម្ពុជាជាប្រទេសកំពុងអភិវឌ្ឍន៍ ហេដ្ឋារចនាសម្ព័ន្ធ ស្តាប់នទន់ខ្សោយ អនក្ខរភាព និងខ្វះការយល់ដឹងពីបច្ចេកវិទ្យាទំនាក់ទំនង និងព័ត៌មាន ជាអាទិ៍ ។ ការកើតឡើងនូវបទល្មើសព័ត៌មានវិទ្យានេះទៀតសោត គឺមានមូលហេតុមូលហេតុទាំងនោះមាននៅ**កថាខណ្ឌទី ២** ខាងក្រោមនេះ ។

កថាខណ្ឌទី ២ មូលហេតុនៃការកើតមានបទល្មើសព័ត៌មានវិទ្យានៅកម្ពុជា

នៅប៉ុន្មានឆ្នាំចុងក្រោយនេះ បច្ចេកវិទ្យានៅព្រះរាជាណាចក្រកម្ពុជា មានការរីកចម្រើនយ៉ាងខ្លាំង ។[12] ទន្ទឹមនឹងការវិវឌ្ឍនៃបច្ចេកវិទ្យា យើងសង្កេតឃើញមានបទល្មើសដែលប្រើប្រាស់បច្ចេកវិទ្យាជាមធ្យោបាយក៏កំពុងកើតមានជាច្រើនករណី និងមានប្រជាជនក្លាយជាជនរងគ្រោះជាបន្តបន្ទាប់ផងដែរ ។ បើយើងសិក្សាឱ្យបានស៊ីជម្រៅ ឃើញថាមូលហេតុដែលធ្វើឱ្យបទល្មើសព័ត៌មានវិទ្យាកើតមានឡើង ដែលមូលហេតុទាំងនោះរួមមាន **កំណើននៃការប្រើប្រាស់បច្ចេកវិទ្យាពីសំណាក់ប្រជាពលរដ្ឋទូទៅ**(២.១) **កង្វះការយល់ដឹងអំពីហានិភ័យនៃការប្រើប្រាស់បច្ចេកវិទ្យា**(២.២) **កត្តាច្បាប់ បទដ្ឋានគតិយុត្ត និងយន្តការពាក់ព័ន្ធនានាដើរពុំទាន់បរិបទនៃបច្ចេកវិទ្យា**(២.៣) **ភាពអំណោយផលនៃប្រតិបត្តិការផ្នែរប្រាក់**(២.៤) ។[13]

២.១ កំណើននៃការប្រើប្រាស់បច្ចេកវិទ្យាពីសំណាក់ប្រជាពលរដ្ឋទូទៅ

យោងតាមរបាយការណ៍ដែលបានចេញផ្សាយដោយ Hootsuite នៅឆ្នាំ២០២០ បានបង្ហាញថាព្រះរាជាណាចក្រកម្ពុជាមានក្រុមហ៊ុនផ្តត់ផ្តង់សេវាអ៊ីនធឺណិតប្រមាណ**៤៧(សែសិបប្រាំពីរ) ក្រុមហ៊ុន** ចំណែកតួលេខនៃការប្រើប្រាស់អ៊ីនធឺណិតមានចំនួន**៨.៨៦(ប្រាំបីកណ្តាក់សញ្ញាប៉ែតសិបប្រាំមួយ)លាននាក់** ស្មើនឹង**៥២.៦%(ហាសិបពីរកណ្តាក់សញ្ញាប្រាំមួយ)ភាគរយ** នៃប្រជាជនកម្ពុជាសរុប ។ រីឯអ្នកប្រើប្រាស់បណ្តាញសង្គមមានចំនួន**១២(ដប់ពីរ)លាននាក់** ស្មើនឹង**៧១.៣%(ចិតសិបមួយកណ្តាក់សញ្ញាបី)ភាគរយ** នៃប្រជាជន កម្ពុជាសរុប ។ ចំពោះការប្រើប្រាស់សេវាទូរស័ព្ទមានប្រមាណ**២១.១៨(ម្ភៃមួយកណ្តាក់សញ្ញាដប់ប្រាំបី)លាននាក់** ស្មើនឹង**១២៥.៨%(មួយរយម្ភៃប្រាំកណ្តាក់សញ្ញាប្រាំបី)ភាគរយ** បើប្រៀបធៀបនឹងចំនួនប្រជាជនកម្ពុជាសរុប។

២.២ កង្វះការយល់ដឹងអំពីហានិភ័យនៃការប្រើប្រាស់បច្ចេកវិទ្យា

នៅកម្ពុជា កង្វះខាតហេដ្ឋារចនាសម្ព័ន្ធនៅតែបន្តចាត់ទុកជាមូលហេតុសំខាន់ដែលបង្កឱ្យកើតមានគម្លាតឌីជីថលនៅក្នុងសង្គម ។ លើសពីនេះ គេនៅសង្កេតឃើញមានគម្លាតឌីជីថលកម្រិតខ្ពស់រវាងប្រជាជនទៅតាមទីជនបទ និងទីក្រុងដោយសារតែការប្រើប្រាស់បច្ចេកវិទ្យា ទាំងនោះមានភាគច្រើននៅតាមតំបន់ទីប្រជុំជន ។ គម្លាតឌីជីថលនេះ បង្កឱ្យមានវិសមភាពនៃការទទួលបានឱកាស និងផលប្រយោជន៍នានា ដែលផ្តល់ឱ្យដោយ

[12] IT.Department.MOI (ចូលទស្សនានៅថ្ងៃទី ១៤ ខែមិថុនា ឆ្នាំ២០២១)។

[13] IT.Department.MOI (ចូលទស្សនានៅថ្ងៃទី ១៤ ខែមិថុនា ឆ្នាំ២០២១)។

បច្ចេកវិទ្យានៅក្នុងសង្គម ។ កង្វះការយល់ដឹងអំពីហានិភ័យនៃការប្រើប្រាស់បច្ចេកវិទ្យា អាចដោយសារមូលហេតុខាងក្រោម៖[14]

- កត្តាអ្នកប្រើប្រាស់
- កត្តាបច្ចេកវិទ្យា
- កត្តាសង្គម

២.៣ កត្តាច្បាប់ បទដ្ឋានគតិយុត្ត និងយន្តការពាក់ព័ន្ធនានាដើរតួនាទីបែបណាលើបច្ចេកវិទ្យា

ដូចបានបញ្ជាក់ជូនមកហើយ កម្ពុជាយើងមានតែក្រមព្រហ្មទណ្ឌទេ ដែលមានចែងអំពីការផ្តន្ទាទោសទៅលើបទល្មើសព័ត៌មានវិទ្យា ក៏ប៉ុន្តែបទបញ្ញត្តិប៉ុណ្ណោះមិនគ្រប់គ្រងទៅបទល្មើសព័ត៌មានវិទ្យានោះ ពោលបច្ចេកវិទ្យាមានការរីកចម្រើនជារៀងរាល់ថ្ងៃ ។ ម្លោះហើយ កម្ពុជាយើងកំពុងតែព្រាងច្បាប់ពីរដែលកម្ពុជាកំពុងត្រូវការគឺច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន និងច្បាប់សន្តិសុខបច្ចេកវិទ្យា ជាដើម ។

២.៤ តារាងអំណោយផលនៃប្រតិបត្តិការផ្ទេរប្រាក់

ក្នុងរយៈពេលប៉ុន្មានឆ្នាំថ្មីៗចំនួនគ្រឹះស្ថានធនាគារ និងហិរញ្ញវត្ថុ និងស្ថាប័នសេវាកម្មទូទាត់នៅក្នុងទីផ្សារទូទាត់បានកើនឡើងគួរឱ្យកត់សម្គាល់ ។[15] នៅខែមិថុនា ឆ្នាំ២០២០ គឺមានស្ថាប័នធនាគារ និងហិរញ្ញវត្ថុចំនួន៣(បី) និងស្ថាប័នផ្តល់សេវាទូទាត់ប្រាក់ចំនួន២៣(ម្ភៃបី) ដែលទទួលបានអាជ្ញាប័ណ្ណដើម្បីផ្តល់សេវាទូទាត់តាមទូរស័ព្ទដៃតាមអ៊ីនធឺណិត ដែលមានលក្ខណៈជាការផ្ទេរមូលនិធិ ការផ្ទេរសាច់ប្រាក់ចូល ឬចេញ ការលក់រាយ ការទូទាត់ថ្លៃទឹក ភ្លើង ការផ្ទេរប្រាក់អន្តរជាតិ និងការបង់ប្រាក់តាមអនឡាញ ។[16] យោងតាមទិន្នន័យដែលចងក្រងដោយធនាគារជាតិនៃកម្ពុជា ការទូទាត់តាមទូរស័ព្ទដៃ និងផ្ទេរប្រាក់ដោយធនាគារ និងស្ថាប័នសេវាកម្មទូទាត់នៅឆមាសទី១ ឆ្នាំ២០២០ មានចំនួន**១១.៩៩%(ដប់មួយកណ្តាក់សញ្ញាកៅសិបប្រាំបួន)ភាគរយ** និង **១៨៣.៤០%(មួយរយសែសិបបីកណ្តាក់សញ្ញាសែសិប) ភាគរយ** នៃផលិតផលក្នុងស្រុកសរុប ។[17]

ម្យ៉ាងវិញទៀត អាចមានមូលហេតុពីរផ្សេងទៀតដែលជាមូលហេតុនៃការកើតមានបទល្មើសព័ត៌មានវិទ្យានៅកម្ពុជា មូលហេតុពីរនោះរួមមាន៖[18]

- ចោរបច្ចេកវិទ្យាប្រើប្រាស់វិធីសាស្ត្រ និងបច្ចេកទេសខ្ពស់ក្នុងការប្រព្រឹត្តបទល្មើស ។

[14]ទីស្តីការគណៈរដ្ឋមន្ត្រី, គោលនយោបាយអភិវឌ្ឍន៍វិស័យទូរគមនាគមន៍បច្ចេកវិទ្យាគមនាគមន៍ និងព័ត៌មាន, (២០២០), ទំព័រទី៨។

[15]ក្រសួងប្រៃសនីយ៍ និងទូរគមនាគមន៍,យុទ្ធសាស្ត្រពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក, (២៥ វិច្ឆិកា ២០២០), ទំព័រទី៥៨។

[16]ក្រសួងប្រៃសនីយ៍ និងទូរគមនាគមន៍,យុទ្ធសាស្ត្រពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក, (២៥ វិច្ឆិកា ២០២០), ទំព័រទី៥៨។

[17]ក្រសួងប្រៃសនីយ៍ និងទូរគមនាគមន៍,យុទ្ធសាស្ត្រពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក, (២៥ វិច្ឆិកា ២០២០), ទំព័រទី៥៨។

[18]IT.Department.MOI (ចូលទស្សនានៅថ្ងៃទី ១៤ ខែមិថុនា ឆ្នាំ២០២១)។

- ចោរបច្ចេកវិទ្យាប្រព្រឹត្តបទល្មើសស្ថិតក្រោមរចនាសម្ព័ន្ធក្រុមមានការចាត់តាំង ។

ផ្នែកទី ២ ក្របខណ្ឌច្បាប់ និងសេចក្តីព្រាងស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន

កថាខណ្ឌទី ១ ក្របខណ្ឌច្បាប់

នៅកម្ពុជាយើង មិនទាន់មានច្បាប់ពិសេស ឬ ច្បាប់ដោយឡែក ដែលចែងអំពីបទល្មើសព័ត៌មានវិទ្យានោះទេ ។ ខណៈពេលច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មានកំពុងស្ថិតនៅជាសេចក្តីព្រាងច្បាប់ ។ ជាងនេះទៅទៀត កម្ពុជាក៏មានមាត្រាមួយចំនួនដែលចែងសម្រាប់ផ្តន្ទាទោសចារីដែលប្រព្រឹត្តបទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យានៅកម្ពុជា ។ បទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យាស្ថិតនៅក្នុង**គន្លឹទី៣ បទល្មើសប្រឆាំងនឹងទ្រព្យសម្បត្តិ មាតិកាទី២ ការប៉ះពាល់ដល់ទ្រព្យសម្បត្តិ ជំពូកទី២ បទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យា នៃក្រមព្រហ្មទណ្ឌកម្ពុជា ឆ្នាំ ២០០៩** ។ បទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យា ដែលមានចែងនៅក្នុងក្រមព្រហ្មទណ្ឌកម្ពុជា ឆ្នាំ២០០៩ ទាំងនោះរួមមាន៖

- មាត្រា ៤២៧ បទចូលទៅដល់ ឬ ស្ថិតនៅនឹងប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យ
- មាត្រា ៤២៨ បទបង្កើតជាឧបសគ្គដល់ដំណើរការនៃប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យ
- មាត្រា ៤២៩ បទបញ្ចូល លុបបំបាត់ ឬ កែប្រែដោយទុច្ចរិតនូវទិន្នន័យ
- មាត្រា ៤៣០ បទចូលរួមក្នុងក្រុមប្រមូលផ្តុំ ឬ ក្នុងសន្និដ្ឋិភាពដើម្បីរៀបចំប្រព្រឹត្តបទល្មើស
- មាត្រា ៤៣១ ការប៉ុនប៉ង
- មាត្រា ៤៣២ ទោសបន្ថែម

យ៉ាងណាមិញ មាត្រាទាំងអស់មិនបានចែងឱ្យមានភាពជាក់លាក់ ច្បាស់លាស់ ហើយពាក្យពេចន៍ដែលមានចែងនៅក្នុងមាត្រាខាងលើនេះ ក៏មិនបានផ្តល់និយមន័យ ។ ល្អីកនេះ ការបកស្រាយអំពីមាត្រាដែលបានបញ្ញត្តអំពីបទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យានេះ យើងនឹងធ្វើបំភ្លឺនៅក្នុង**ជំពូកទី២** ខាងក្រោម ។

កថាខណ្ឌទី ២ សេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន

នៅពាក់កណ្តាលឆ្នាំ២០១០ ទីស្តីការគណៈរដ្ឋមន្ត្រី បានបង្កើតក្រុមការងារមួយ ដើម្បីបំពេញការងារតាក់តែងសេចក្តីព្រាងច្បាប់នេះ ដោយមានអ្នកជំនាញការខាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន ពីក្រុមប្រឹក្សាអឺរ៉ុប គឺលោក **Alexander Segar** ប្រធានផ្នែកឧក្រិដ្ឋកម្មសេដ្ឋកិច្ច ចូលរួមសហការ ។[19] បន្ថែមពីនេះ ការតាក់តែងសេចក្តីព្រាងច្បាប់ ក៏មានការសហការពីប្រទេសមួយចំនួន តួយ៉ាងប្រទេសថៃ ឥណ្ឌូណេស៊ី ហ្វីលីពីន

[19]សេចក្តីបំភ្លឺទាក់ទងនឹងសេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន, លេខ ៦៥៧ បទ, ២៥ ឧសភា ២០១៥, កថាខណ្ឌទី១ វាក្យខណ្ឌទី១ ចំណុចទី១។

អូស្ត្រាលី និងប្រទេសណូវែលហ្សេឡង់ ។[20] ទៀតសោតនោះ សេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន ត្រូវបានតាក់តែងក្នុងឆ្នាំ២០១៦ ហើយបានជួបប្រជុំពិភាក្សាជាបន្តបន្ទាប់ចំនួន**៦៧(ហុកសិបប្រាំពីរ)លើក**រួចមកហើយ(គិតត្រឹមថ្ងៃទី២៥ ខែកញ្ញា ឆ្នាំ២០២០) ដោយមានការប្រជុំអន្តរក្រសួង នាយកដ្ឋានជំនាញរបស់ក្រសួងមហាផ្ទៃ ព្រមទាំងមានជំនួយឧបត្ថម្ភផ្នែកបច្ចេកទេសពីក្រសួងយុត្តិធម៌នៃសហរដ្ឋអាមេរិក ផងដែរ ។[21] កម្ពុជាយើងបច្ចុប្បន្ននេះ កំពុងតែខិតខំប្រឹងប្រែងបង្កើតច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន ពោលគឺដើម្បីអាចធានាសុចរិតភាពនៃការប្រើប្រាស់ ការគ្រប់គ្រងប្រព័ន្ធកុំព្យូទ័រ ទិន្នន័យ កុំព្យូទ័រ និងការពារសន្តិសុខសណ្តាប់ធ្នាប់សាធារណៈ ព្រមទាំងការការពារសិទ្ធិសេរីភាពបុគ្គល ដើម្បីបង្ការ ទប់ស្កាត់ និងបង្ក្រាបបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន។ សេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាននេះមាន**៦(ប្រាំមួយ)ជំពូក និង៤០(សែសិប)មាត្រា** ។ បន្ថែមពីនេះ យើងសូមលើកយកសេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មានដោយបែងចែកជា៤(បួន)ចំណុចទៀតដែលក្នុងនោះរួមមាន **គោលបំណងនិងគោលដៅ**(២.១) **រចនាសម្ព័ន្ធនៃសេចក្តីព្រាងច្បាប់**(២.២) **បទល្មើស**(២.៣) និង**ជំនួយផ្នែកច្បាប់ទៅវិញទៅមកនិងកិច្ចសហប្រតិបត្តិការអន្តរជាតិនិងបត្យាប័ន**(២.៤)។

២.១ គោលបំណង និងគោលដៅ

សេចក្តីព្រាងច្បាប់នេះ មានគោលបំណងកំណត់វិធានការអប់រំ បង្ការទប់ស្កាត់ និងបង្ក្រាបការប្រព្រឹត្តអំពើល្មើសនានា តាមប្រព័ន្ធបច្ចេកវិទ្យា ។[22]

សេចក្តីព្រាងច្បាប់នេះ មានគោលដៅធានាការអនុវត្តច្បាប់ ប្រយុទ្ធប្រឆាំង និងបង្ក្រាបរាល់បទល្មើសតាមប្រព័ន្ធបច្ចេកវិទ្យា ព្រមទាំងមានគោលដៅ ក្នុងការធានាសុវត្ថិភាព និងការពារផលប្រយោជន៍ស្របច្បាប់ក្នុងការប្រើប្រាស់និងអភិវឌ្ឍន៍បច្ចេកវិទ្យា ។[23]

២.២ រចនាសម្ព័ន្ធនៃសេចក្តីព្រាងច្បាប់

ដូចបានជម្រាបជូនខាងលើហើយថា សេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាត្រូវបានបែងចែកជា ៦(ប្រាំមួយ)ជំពូក ដែលជំពូកទី១ បញ្ញត្តិទូទៅ ដែលមានចែងអំពី គោលបំណង និងគោលដៅ។ រីឯជំពូកទី២ គណៈកម្មាធិការជាតិប្រឆាំងបទល្មើសតាមប្រព័ន្ធបច្ចេកវិទ្យា ដែលមានចែងអំពីការបង្កើតគណៈកម្មាធិការ

[20]សេចក្តីបំភ្លឺទាក់ទងនឹងសេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន, លេខ ៦៥៧ បទ, ២៥ ឧសភា ២០១៥, កថាខណ្ឌទី១ វាក្យខណ្ឌទី២ នៃចំណុចទី១។

[21]https://www.information.gov.kh/articles/14898 (ចូលមើលថ្ងៃ ១០ ខែមិថុនា ឆ្នាំ២០២១)។

[22]សេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន, ២០១៦, មាត្រា១។

[23]សេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន, ២០១៦, មាត្រា២។

ប្រឆាំងនឹងបទល្មើសតាមប្រព័ន្ធបច្ចេកវិទ្យា(មាត្រា៥) សមាសភាព(មាត្រា៦) ភារកិច្ច(មាត្រា៧) អគ្គលេខាធិការដ្ឋាន គ.ប.ប(មាត្រា៨) ភារកិច្ចអគ្គលេខាធិការដ្ឋាន នៃគ.ប.ប(មាត្រា៩) មន្ត្រីនៃអគ្គលេខាធិការដ្ឋានៃគ.ប.ប (មាត្រា១០) និងបណ្តាញនៃអគ្គលេខាធិការដ្ឋាន គ.ប.ប(មាត្រា១១) ។ ចំណែកឯជំពូកទី៣ នីតិវិធីសម្រាប់អនុវត្តចំពោះបទល្មើសបច្ចេកវិទ្យា(មាត្រា១៣) មន្ត្រីមានសមត្ថកិច្ចនៅក្នុងការស៊ើបអង្កេតបទល្មើសបច្ចេកវិទ្យា (មាត្រា១៤) ការផ្តល់នីតិសម្បទានចំពោះមន្ត្រីនៃអគ្គលេខាធិការដ្ឋាន គ.ប.ប(មាត្រា១៥) អំណាចស៊ើបអង្កេតរបស់អគ្គលេខាធិការដ្ឋាន គ.ប.ប(មាត្រា១៦) ការរក្សាទុកទិន្នន័យកុំព្យូទ័រនិងចរាចរណ៍ទិន្នន័យ(មាត្រា១៧) ការថតចម្លងទិន្នន័យ (មាត្រា១៨) ការស្វែងរកការរឹបអូសទិន្នន័យកុំព្យូទ័រ(មាត្រា១៩) និងលក្ខខណ្ឌនិងការការពារ(មាត្រា២០) ។ ចំពោះជំពូកទី៤ បទល្មើស នៅជំពូកនេះមានចែងអំពីការភ្ជាប់ដោយខុសច្បាប់ (មាត្រា២១) ចារកម្មទិន្នន័យ(មាត្រា២២) ការស្ទាក់ចាប់ដោយខុសច្បាប់(មាត្រា២៣) ការជ្រៀតជ្រែកទិន្នន័យ (មាត្រា២៤) ការផ្ទេរទិន្នន័យដោយគ្មានការអនុញ្ញាត(មាត្រា២៥) រូបភាពអាសអាភាសកុមារ(មាត្រា២៧) ខ្លឹមសារនិងគេហទំព័រ(មាត្រា២៨) កម្មសិទ្ធិបញ្ញា(មាត្រា២៩) ការឆបោកតាមរយៈកុំព្យូទ័រ(មាត្រា៣០) ការក្លែងបន្លំតាមរយៈកុំព្យូទ័រ(មាត្រា៣១) ការប្រើឧបករណ៍ក្នុងផ្លូវខុស(មាត្រា៣២) ជាអាទិ៍ ។ ទៀតសោធនោះ ជំពូកទី៥ ជំនួយផ្នែកច្បាប់ទៅវិញទៅមកនិងកិច្ចសហប្រតិបត្តិការអន្តរជាតិនិងបត្យាប័ន ជំពូកនេះមានចែងអំពីបទប្បញ្ញត្តិដែលត្រូវអនុវត្តក្នុងរឿងបត្យាប័ន(មាត្រា៣៦) ជំនួយផ្នែកច្បាប់ទៅវិញទៅមកក្នុងករណីបទល្មើសដែលមានចែងក្នុងច្បាប់នេះ(មាត្រា៣៧) និងនីតិវិធីជំនួយផ្នែកច្បាប់ទៅវិញទៅមក(មាត្រា៣៨)។ ចុងក្រោយនោះគឺ ជំពូកទី៦ អវសានប្បញ្ញត្តិ។

ចំណុចសំខាន់ដែលយើងគួរគប្បីសិក្សាបន្ថែមនោះគឺ នៅក្នុងសេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន បានបញ្ញត្តអំពីការបង្កើតគណៈកម្មាធិការជាតិប្រឆាំងនឹងបទល្មើសតាមប្រព័ន្ធបច្ចេកវិទ្យាដែលសមាសភាពរបស់គណៈកម្មាធិការជាតិប្រឆាំងនឹងបទល្មើសតាមប្រព័ន្ធបច្ចេកវិទ្យា មានដូចតទៅ៖[24]

- នាយករដ្ឋមន្ត្រី ជាប្រធាន
- ឧបនាយករដ្ឋមន្ត្រី រដ្ឋមន្ត្រីទទួលបន្ទុកទីស្តីការគណៈរដ្ឋមន្ត្រី អនុប្រធាន
- រដ្ឋលេខាធិការក្រសួងមហាផ្ទៃ សមាជិក
- រដ្ឋលេខាធិការក្រសួងព័ត៌មាន សមាជិក
- រដ្ឋលេខាធិការក្រសួងប្រៃសណីយ៍ និងទូរគមនាគមន៍ សមាជិក
- រដ្ឋលេខាធិការក្រសួងយុត្តិធម៌ សមាជិក

[24]សេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន, ២០១៦, មាត្រា៦។

- រដ្ឋលេខាធិការក្រសួងការបរទេស សមាជិក
- អគ្គស្នងការនគរបាលជាតិ សមាជិក
- តំណាងគណៈកម្មាធិការជាតិប្រឆាំងអំពីការរកម្ម សមាជិក
- អគ្គលេខាធិការ NiDA សមាជិក
- តំណាងក្រុមប្រឹក្សាអ្នកច្បាប់ នៃទីស្តីការគណៈរដ្ឋមន្ត្រី សមាជិក
- តំណាងក្រុមប្រឹក្សាសេដ្ឋកិច្ច សង្គមកិច្ច និងវប្បធម៌ សមាជិក
- តំណាងសភាពាណិជ្ជកម្មកម្ពុជា សមាជិក
- អគ្គលេខាធិការនៃ គ.ប.ប សមាជិកអចិន្ត្រៃយ៍

១.៣ បទល្មើស

នៅក្នុងសេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន បានចែងបទល្មើសបានច្បាស់លាស់ជាងបទល្មើសដែលបានចែងនៅក្នុងបទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យា ដែលមានចែងនៅក្នុងក្រមព្រហ្មទណ្ឌ ឆ្នាំ២០០៩ ។ បទល្មើសដែលមានចែងនៅក្នុងសេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន រួមមានការភ្ជាប់ដោយខុសច្បាប់ ចារកម្មទិន្នន័យ ការស្ទាក់ចាប់ដោយខុសច្បាប់ ការជ្រៀតជ្រែកទិន្នន័យ ការផ្ទេរទិន្នន័យដោយគ្មានការអនុញ្ញាត ការជ្រៀតជ្រែកប្រព័ន្ធ រូបភាពអាសអាភាស ការឆបោកតាមរយៈកុំព្យូទ័រ ការក្លែងបន្លំតាមរយៈ កុំព្យូទ័រ ការប្រើឧបករណ៍ក្នុងផ្លូវខុស ការប៉ុនប៉ង ទោសបន្ថែមចំពោះរូបវន្តបុគ្គល និងទោសបន្ថែមចំពោះនីតិបុគ្គល ។

១.៤ ជំនួយផ្នែកច្បាប់ទៅវិញទៅមកនិងកិច្ចសហប្រតិបត្តិការអន្តរជាតិ និងបត្យាប័ន

សេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មានបានចែងថា បទប្បញ្ញត្តិនៃជំពូកទី២ មាតិកាទី១ គន្លឹទី៩ នៃក្រមនីតិវិធីព្រហ្មទណ្ឌ ត្រូវយកមកអនុវត្តក្នុងរឿងបត្យាប័នទាក់ទងនឹងបទល្មើសដែលមានចែងនៅក្នុងសេចក្តីព្រាងច្បាប់នេះ ។ ជាងនេះទៅទៀត អាជ្ញាធរតុលាការ នៃព្រះរាជាណាចក្រកម្ពុជាអាចប្រគល់អំណាចឱ្យទៅអាជ្ញាធរខាងតុលាការមានសមត្ថកិច្ចនៃរដ្ឋបរទេសណាមួយ និងអាចទទួលអំណាចពីអាជ្ញាធរតុលាការនៃរដ្ឋបរទេសណាមួយដែរ ពោលគឺដើម្បីៈ [25]

- ផ្តល់ព័ត៌មាន និងវត្ថុតាង
- ធ្វើការត្រួតពិនិត្យវត្ថុតាង និងទីកន្លែង
- ធ្វើការឆែកឆេរ ឃាត់ទុក និងដកហូត
- ឱ្យដំណឹងពីលិខិតផ្សេងៗ របស់តុលាការ

[25]សេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន, ២០១៦, មាត្រា ៣៧។

- ឱ្យដំណឹងអំពីការចោទប្រកាន់តាមនីតិវិធីព្រហ្មទណ្ឌ
- រកឱ្យឃើញ និងកំណត់អត្តសញ្ញាណសាក្សី និងជនសង្ស័យ
- ប្រមូលយកសក្ខីភាព ឬ យកចម្លើយដែលឆ្លើយតាមផ្លូវតុលាការ
- បញ្ជាឱ្យធ្វើការរឹបអូសវត្ថុទាំងឡាយដែលមានចែងក្នុងចំណុចខាងលើ
- ផ្តល់ឯកសារកំណត់ហេតុច្បាប់ដើម ឬសេចក្តីចម្លងដោយបញ្ជាក់ត្រឹមត្រូវតាមច្បាប់ដើមនៃឯកសារ និងសំណុំរឿងរាប់ទាំងសេចក្តីស្រង់បញ្ជី ប្រាក់ពីធនាគារ ឯកសារគណនេយ្យ សំណុំរឿងរបស់ក្រុមហ៊ុន និងឯកសារពាណិជ្ជកម្ម ព្រមទាំងលិខិតយថាភូត ឬ លិខិតឯកជន
- ដាក់ក្រោមវិធានការរក្សាទុកជាបណ្តោះអាសន្ននូវផលិតផល និងទ្រព្យសម្បត្តិដែលបានមកពីបទល្មើសបច្ចេកវិទ្យាទាំងបរិក្ខារសម្ភារៈ ឬ ទុកសម្រាប់ប្រើប្រាស់ដើម្បីប្រព្រឹត្តបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន
- បង្ហាញ ឬ ផ្តល់សាក្សីអ្នកជំនាញ ឬ ជនដទៃទៀត រាប់ទាំងជនឃុំខ្លួន ដែលយល់ព្រមផ្តុយក្នុងការស៊ើបអង្កេត ឬ យល់ព្រមចូលរួមក្នុងនីតិវិធី
- កំណត់អត្តសញ្ញាណ ឬស្រាវជ្រាវរកធនធាន ទ្រព្យសម្បត្តិ បរិក្ខារ និងសម្ភារៈទាំងឡាយដែលបានមក

នីតិវិធីនៃការអនុវត្តជំនួយផ្នែកច្បាប់ទៅវិញទៅមក ត្រូវអនុវត្តតាមគោលការណ៍ទាំងឡាយដែលបានកំណត់ក្នុងសន្ធិសញ្ញា ឬ កិច្ចព្រមព្រៀងទ្វេភាគី និងពហុភាគី និងច្បាប់ជាតិជាធរមាន។[26]

[26]សេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន, ២០១៦, មាត្រា ៣៨។

ជំពូកទី ២
បទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យា និងស្ថាប័នជំនាញ

យើងសង្កេតឃើញថាបច្ចុប្បន្នករណីដែលមានការលួចចូលក្នុងទិន្នន័យឯកជនភាពរបស់បុគ្គលដទៃទៀត កំពុងតែកើតមានឡើងជាបន្តបន្ទាប់ ។[27] បន្ថែមពីនោះមិនត្រឹមតែការលួចចូលក្នុងទិន្នន័យឯកជនប៉ុណ្ណោះទេ ចោរបច្ចេកវិទ្យាថែមទាំងលួចយកទិន្នន័យទាំងនោះ ទៅប្រើប្រាស់ក្រោមរូបភាពជាបទល្មើសឆបោក ឬ ចាប់ជំរិតទាមទារប្រាក់ ជាអាទិ៍ ដែលបណ្តាលឱ្យមានភាពរឹករឹងក្នុងសង្គម ក៏ដូចជាប៉ះពាល់យ៉ាងធ្ងន់ធ្ងរដល់ម្ចាស់ទិន្នន័យជាអាទិ៍ ។ បទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យា មានចែងក្នុងក្រមព្រហ្មទណ្ឌ នៃព្រះរាជាណាចក្រកម្ពុជាដែលនៅជាធរមាន ។ គួសបញ្ជាក់ថា បទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យា គឺមានស្ថានភាពខុសពីបទល្មើសផ្សេងៗទៀត ត្រង់ថាកន្លែងដែលកើតមាននូវបទល្មើសគឺស្ថិតនៅលើប្រព័ន្ធបច្ចេកវិទ្យា រួមទាំងភស្តុតាងជាអាទិ៍ ដោយចារីមិនបានបង្ហាញមុខនៅកន្លែងកើតហេតុនោះទេ ។ ល្ងឹកនេះគឺទាមទារឱ្យមានស្ថាប័នជំនាញដើម្បីឆ្លើយតបទៅនឹងបញ្ហានេះ ។ ហេតុនេះហើយ នៅក្នុងជំពូកទី២នេះ យើងនឹងសិក្សាអំពី**បទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យា**(ផ្នែកទី១) និង**ស្ថាប័នជំនាញ**(ផ្នែកទី២) ។

ផ្នែកទី ១ បទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យា

នៅក្នុងក្រមព្រហ្មទណ្ឌ ឆ្នាំ២០០៩ បានបញ្ញត្តអំពីបទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យា ដែលមានមាត្រាចំនួន៦(ប្រាំមួយ) ។ មាត្រាទាំងនោះចែងអំពី **បទចូលទៅដល់ ឬ ស្ថិតនៅនឹងប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យ**(កថាខណ្ឌទី១) **បទបង្កើតជាឧបសគ្គដល់ដំណើរការនៃប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យ**(កថាខណ្ឌទី២) **បទបញ្ចូល លុបបំបាត់ ឬ កែប្រែដោយទុច្ចរិតនូវទិន្នន័យ**(កថាខណ្ឌទី៣) **បទចូលរួមក្នុងក្រុមប្រមូលផ្តុំ ឬ ក្នុងសន្និដ្ឋិភាពដើម្បីរៀបចំប្រព្រឹត្តបទល្មើស**(កថាខណ្ឌទី៤) **ការប៉ុនប៉ង**(កថាខណ្ឌទី៥) និង**ទោសបន្ថែម**(កថាខណ្ឌទី៦) ។ មុននឹងធ្វើការបកស្រាយទៅលើផ្នែកទី១នេះ យើងសូមគួសបញ្ជាក់ថា ក្រមព្រហ្មទណ្ឌ កម្ពុជាឆ្នាំ២០០៩ មិនបានចែងឱ្យបានច្បាស់លាស់ ព្រមទាំងពន្យល់ និងបកស្រាយនិយមន័យថាអ្វីទៅជាប្រព្រឹត្តិកម្មស្វ័យប្រវត្តិនៃទិន្នន័យឡើយ ។ សូមបញ្ជាក់ថា ក្នុងរឿងព្រហ្មទណ្ឌ ច្បាប់ត្រូវបកស្រាយយ៉ាងតឹងរឹង ។[28] ម្ល៉ោះហើយ ប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យ សំដៅដល់កម្មវិធីកុំព្យូទ័រ ប្រព័ន្ធកុំព្យូទ័រ ប្រព័ន្ធ ឬ បណ្តាញអេឡិចត្រូនិក ឬ មធ្យោបាយអេឡិចត្រូនិកផ្សេងទៀតដែលត្រូវបានប្រើប្រាស់សម្រាប់ជូនដំណឹង ឬ ឆ្លើយតប ។[29]

[27] https://www.interior.gov.kh/news/detail/2002 (ចូលទស្សនានៅថ្ងៃទី ១២ ខែមិថុនា ឆ្នាំ២០២១)។

[28] ក្រមព្រហ្មទណ្ឌ, លេខ នស/រកម/១២០៧/០៣០, ០៨ ធ្នូ ២០០៩, មាត្រា ៥។

[29] ច្បាប់ស្តីពីពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក, លេខ នស/រកម/១១១៩/០១៧, ០២ វិច្ឆិកា ២០១៩, ចំណុចទី ៣, ទំព័រទី២៤។

កថាខណ្ឌទី ១ បទចូលទៅដល់ ឬ ស្ថិតនៅនឹងប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យ

ជាគោលការណ៍ ដើម្បីចាត់ទុកថាអំពើមួយជាបទល្មើស គឺត្រូវបំពេញនូវធាតុផ្សំបីគឺ **ធាតុនីត្យានុកូល**(១.១) **ធាតុសត្យានុម័ត**(១.២) និង**ធាតុអត្តនោម័ត**(១.២) ។

១.១ ធាតុនីត្យានុកូល

មុននឹងធ្វើការបកស្រាយ យើងសូមលើកឡើងនូវទ្រឹស្តីដែលមានចែងនៅក្នុងក្រមព្រហ្មទណ្ឌ ។ ក្រមនេះបានចែងថា មានតែអំពើដែលបង្កើតជាបទល្មើស នៅពេលដែលអំពើនោះមានចែងក្នុងបទប្បញ្ញត្តិព្រហ្មទណ្ឌជាធរមានប៉ុណ្ណោះ ទើបត្រូវផ្តន្ទាទោសព្រហ្មទណ្ឌបាន ។[30] មានតែទោសដែលមានចែងក្នុងបទប្បញ្ញត្តិព្រហ្មទណ្ឌជាធរមាន នៅពេលដែលបទល្មើស ត្រូវបានប្រព្រឹត្តប៉ុណ្ណោះ ទើបអាចត្រូវប្រកាសបាន ។[31]

បទចូលទៅដល់ ឬ ស្ថិតនៅនឹងប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យ មានចែងនៅក្នុងមាត្រា៤២៧ នៃក្រមព្រហ្មទណ្ឌកម្ពុជា ឆ្នាំ២០០៩ ។ ក្រមនេះបានចែងថា អំពើចូលទៅដល់ ឬ ស្ថិតនៅនឹងប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យ ដោយទុច្ចរិត ត្រូវផ្តន្ទាទោសដាក់ពន្ធនាគារពី ១ (មួយ) ខែ ទៅ ១ (មួយ) ឆ្នាំ និងពិន័យជាប្រាក់ពី ១០០.០០០ (មួយសែន) រៀល ទៅ ២.០០០.០០០ (ពីរលាន) រៀល ។[32]

ម្យ៉ាងវិញទៀត បើក្នុងករណីអំពើនោះបណ្តាលឱ្យមានការលុបបំបាត់ ឬ កែប្រែទិន្នន័យដែលមាននៅក្នុងប្រព័ន្ធ ឬ ឱ្យមានការខូចខាតនូវដំណើរការនៃប្រព័ន្ធ បទល្មើសនេះត្រូវផ្តន្ទាទោសដាក់ពន្ធនាគារ ១ (មួយ) ឆ្នាំ ទៅ ២ (ពីរ) ឆ្នាំ និងពិន័យជាប្រាក់ពី ២.០០០.០០០ (ពីរលាន) រៀលទៅ ៤.០០០.០០០ (បួនលាន) រៀល ។[33]

១.២ ធាតុសត្យានុម័ត

នៅក្នុងធាតុសត្យានុម័តចំពោះ បទចូលទៅដល់ ឬ ស្ថិតនៅនឹងប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យ យើងនឹងលើកឡើងអំពី៖ **អំពើ** (១.២.១) **ព្យសនកម្ម**(១.២.២) និង**ទំនាក់ទំនងហេតុនិងផល**(១.២.៣)។

១.២.១ អំពើ

ចំពោះអំពើរបស់ចារីដែលបានប្រព្រឹត្តបទល្មើសគឺជាអំពើសកម្ម ពោលយើងអាចសង្កេតឃើញសត្យានុម័តនៃសកម្មភាពដែលចារីចូលទៅដល់ ឬ ស្ថិតនៅនឹងប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យ ។ តើសកម្មដែលចារីចូលទៅដល់ ឬ ស្ថិតនៅនឹងប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យ នោះយ៉ាងដូចម្តេច?

- អំពើចូលទៅដល់ប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យ ៖ មានន័យថាចារីបានប្រើប្រាស់ឧបករណ៍

[30]ក្រមព្រហ្មទណ្ឌ, លេខ នស/រកម/១២០៧/០៣០, ០៨ ធ្នូ ២០០៩, កថាខណ្ឌទី១ នៃមាត្រា ៣។

[31]ក្រមព្រហ្មទណ្ឌ, លេខ នស/រកម/១២០៧/០៣០, ០៨ ធ្នូ ២០០៩, កថាខណ្ឌទី២ នៃមាត្រា ៣។

[32]ក្រមព្រហ្មទណ្ឌ, លេខ នស/រកម/១២០៧/០៣០, ០៨ ធ្នូ ២០០៩, កថាខណ្ឌទី១ នៃមាត្រា ៤២៧។

[33]ក្រមព្រហ្មទណ្ឌ, លេខ នស/រកម/១២០៧/០៣០, ០៨ ធ្នូ ២០០៩, កថាខណ្ឌទី២ នៃមាត្រា ៤២៧។

អេឡិចត្រូនិក ដូចជា កុំព្យូទ័រ ឬ ទូរស័ព្ទ ហែកចូលទៅដល់ប្រព័ន្ធប្រព្រឹត្តិកម្មស្ងួយប្រវត្តនៃទិន្នន័យរបស់ជនរងគ្រោះ ។ គួសបញ្ជាក់ថា នៅទីនេះយើងមិនធ្វើការបកស្រាយអំពីបច្ចេកទេសនៃការហែកនោះទេ ហើយយើងគ្រាន់តែចង់បញ្ជាក់សកម្មភាពរបស់ចារីក្នុងការប្រព្រឹត្តបទល្មើស គឺទាល់តែចារីនោះមានចំណេះដឹងទាក់ទងទៅនឹងវិស័យព័ត៌មានវិទ្យា ។

- ស្ថិតនៅក្នុងប្រព័ន្ធប្រព្រឹត្តិកម្មស្ងួយប្រវត្តនៃទិន្នន័យ ៖ មានន័យថាក្រោយសកម្មភាពដែលចារីបានចូលទៅដល់ប្រព័ន្ធប្រព្រឹត្តិកម្មស្ងួយប្រវត្តនៃទិន្នន័យរបស់ជនរងគ្រោះ ចារីបន្តស្ថិតនៅក្នុងប្រព័ន្ធប្រព្រឹត្តិកម្មស្ងួយប្រវត្តនៃទិន្នន័យ ។ ក្នុងអំឡុងពេលស្ថិតនៅក្នុងប្រព័ន្ធប្រព្រឹត្តិកម្មស្ងួយប្រវត្តនៃទិន្នន័យ ចារីអាចធ្វើសកម្មភាពឆែកមើលទិន្នន័យរបស់ជនរងគ្រោះដូចជា លេខកុងធនាគារ ព័ត៌មានសម្ងាត់ផ្ទាល់ខ្លួន ជាអាទិ៍ ។

ចំណាំ៖ នៅពេលដែលចារីចូល ឬ ស្ថិតនៅក្នុងប្រព័ន្ធប្រព្រឹត្តិកម្មស្ងួយប្រវត្តនៃទិន្នន័យ អំពើទាំងនោះអាចបណ្តាលឱ្យមានការលុបបំបាត់ ឬ កែប្រែទិន្នន័យរបស់ជនរងគ្រោះថែមទៀតផង ។ ឧទាហរណ៍ **លោក សៀងហៃ** បានប្រើប្រាស់កុំព្យូទ័រដើម្បីធ្វើការហែកចូលកុំព្យូទ័ររបស់ **លោក ខ** ហើយការហែកចូលនោះ បានបណ្តាលឱ្យមានការបាត់នូវទិន្នន័យដែលមាននៅក្នុងកុំព្យូទ័រ**របស់ លោក ខ** ។

១.២.២ ព្យសនកម្ម

បើនិយាយអំពីព្យសនកម្មនៃបទល្មើសនេះ អាចមានទាំងព្យសនកម្មផ្លូវចិត្ត ព្យសនកម្មផ្នែកសម្ភារៈ និងព្យសនកម្មដល់សន្តិសុខសណ្តាប់ធ្នាប់សាធារណៈ ហើយជាទូទៅមិនមានព្យសនកម្មផ្លូវកាយនោះទេ ដោយហេតុថាបទល្មើសនេះ ចារីមិនបានប្រើអំពើហិង្សា ទៅលើជនរងគ្រោះ ជាអាទិ៍ឡើយ ។ ឧទាហរណ៍ **លោក សៀងហៃ** បានប្រើប្រាស់កុំព្យូទ័រដើម្បីហែកចូលក្នុងកុំព្យូទ័ររបស់ក្រសួងមហាផ្ទៃ ហើយបណ្តាលឱ្យមាននូវការលុបបំបាត់ ឬ កែប្រែនូវទិន្នន័យ ដូចបានលើកឡើងនៅជំពូកទី១ ។ ហេតុនេះព្យសនកម្មនឹងអាចកើតមាន៖

១- ផ្លូវចិត្តរបស់រូបវន្តបុគ្គលនៃស្ថាប័ន ។

២- ការហែកចូលរបស់ចារី បង្កឱ្យមានការខូចខាតដល់ទិន្នន័យដែលមាននៅកុំព្យូទ័ររបស់ក្រសួង និង

៣-ប្រសិនបើឯកសារនោះទាក់ទងនឹងរឿងសំខាន់ ដូចជាការបញ្ជាទិញអាវុធពីក្រៅប្រទេសជាអាទិ៍ ហើយត្រូវបានលុប ឬ កែប្រែ ដូច្នេះនឹងបង្កនូវព្យសនកម្មដល់សណ្តាប់ធ្នាប់សាធារណៈ នៅពេលដែលទិន្នន័យទាំងនោះត្រូវបានបង្ហាញជាសាធារណៈ ។

១.២.៣ ទាក់ទងហេតុ និងផល

ចំណងទាក់ទងហេតុ និងផលនៃបទល្មើសនេះ តាមឧទាហរណ៍ទី២ខាងលើ ប្រសិនបើ **លោក សៀងហៃ** មិនធ្វើការហែកចូលកុំព្យូទ័ររបស់ក្រសួងមហាផ្ទៃទេ នោះក៏គ្មានព្យសនកម្មកើតមានឡើងដែល ឬ និយាយម្យ៉ាងទៀតថា ព្យសនកម្មមិនកើតមាននោះទេ ប្រសិនបើ **លោក សៀងហៃ** មិនហែកចូលកុំព្យូទ័រ ដែលបណ្តាលឱ្យ

មាននូវការលុបបំបាត់ ឬ កែប្រែទិន្នន័យរបស់ក្រសួងមហាផ្ទៃ ។

១.២ ឆាតុអត្តនោម័ត

ក្រមព្រហ្មទណ្ឌកម្ពុជាបានបញ្ញត្តថា ពុំមានបទល្មើសទេ ប្រសិនបើគ្មានចេតនាប្រព្រឹត្ត ។[34] លើសពីនេះ ក្រមនេះបានចែងថា អំពើចូលទៅដល់ ឬ ស្ថិតនៅនឹងប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យដោយទុច្ចរិត ។ ពាក្យទុច្ចរិតនេះ បញ្ជាក់អំពីកំហុសជាចេតនារបស់ចារី មានន័យថាចារីមានចេតនាទុច្ចរិតចូល ឬ ស្ថិតនៅក្នុងប្រព័ន្ធប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យរបស់ជនរងគ្រោះ ។ គោលដៅរបស់ចារី គឺដើម្បីចូលទៅក្នុង ឬ ស្ថិតនៅនឹងប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យរបស់ជនរងគ្រោះ ដែលចារីអាចនឹងធ្វើការឆែកមើលទិន្នន័យរបស់ជនរងគ្រោះដោយទុច្ចរិត ។ ឧទាហរណ៍ **លោក ពិសិដ្ឋ** បានប្រើប្រាស់កុំព្យូទ័រដើម្បីហែកចូលនៅក្នុងកុំព្យូទ័ររបស់ **លោក សំរិត** ក្នុងចេតនាចូលទៅមើល និងស្រង់យកទិន្នន័យសំខាន់ៗ ដូចជាទិន្នន័យដែលទាក់ទៅនឹងជំនួញជួញដូររបស់ **លោក សំរិត** ជាអាទិ៍ ។

កថាខណ្ឌទី ២ បទបង្កើតជាឧបសគ្គដល់ដំណើរការនៃប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្ត នៃទិន្នន័យ

នៅក្នុងកថាខណ្ឌនេះយើងសង្កេតឃើញពាក្យ ឧបសគ្គ ។ ឧបសគ្គ សំដៅទៅដល់ ឧបទ្រព ចង្រៃ គ្រឿងទើសទាក់ គ្រឿងជំទាស់ គ្រឿងរារាំងដំណើរ ។[35] លើសពីនេះ យើងក៏នឹងសិក្សាបន្តទៀតផងដែលទាក់ទងទៅនឹងធាតុផ្សំនៃបទល្មើស ។

២.១ ឆាតុនីត្សាឧក្ខល

បទបង្កើតជាឧបសគ្គដល់ដំណើរការនៃប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យមានចែងនៅក្នុងមាត្រា ៤២៨ នៃក្រមព្រហ្មទណ្ឌកម្ពុជា ឆ្នាំ២០០៩ ។ ក្រមនេះបានបញ្ញត្តថា អំពើបង្កើតជាឧបសគ្គ ធ្វើឱ្យខូចដំណើរការនៃប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យ ត្រូវផ្តន្ទាទោសដាក់ពន្ធនាគារពី ១ (មួយ) ឆ្នាំ ទៅ ២ (ពីរ) ឆ្នាំ និងពិន័យជាប្រាក់ពី ២.០០០.០០០ (ពីរលាន) រៀល ទៅ ៤.០០០.០០០ (បួនលាន) រៀល ។[36]

២.២ ឆាតុសត្សាឧម័ត

២.២.១ អំពើ

ទាក់ទងនឹងអំពើរបស់ចារីក្នុងបទល្មើសនេះ គឺជាអំពើសកម្ម ច្បាស់ណាស់ចារីគឺបានដឹងអំពីអំពើរបស់ខ្លួន ព្រោះអំពើនេះច្បាប់បានហាមឃាត់ ។ ឧទាហរណ៍ **លោក ចំរើន** បានបង្កើតតំណភ្ជាប់ដែលផ្ទុកទៅដោយមេរោគ

[34]ក្រមព្រហ្មទណ្ឌ, លេខ នស/រកម/១២០៧/០៣០, ០៨ ធ្នូ ២០០៩, កថាខណ្ឌទី១ នៃមាត្រា ៤។

[35]សម្តេចព្រះសង្ឃរាជ ជួនណាត, វចនានុក្រមខ្មែរ, ការផ្សព្វផ្សាយរបស់ពុទ្ធសាសនបណ្ឌិត្យ, ឆ្នាំ១៩៦៨។

[36]ក្រមព្រហ្មទណ្ឌ, លេខ នស/រកម/១២០៧/០៣០, ០៨ ធ្នូ ២០០៩, មាត្រា ៤២៨។

ហើយបានផ្ញើឱ្យ **កញ្ញា សុខា** ។ បន្ទាប់មក **កញ្ញា សុខា** បានចុចទៅលើតំណភ្ជាប់នោះ ដែលជាហេតុធ្វើឱ្យទូរស័ព្ទរបស់ **កញ្ញា សុខា** គាំងលែងដំណើរការ ។

២.២.២ ព្យសនកម្ម

ទាក់ទងទៅនឹងព្យសនកម្មដែលកើតឡើងពីបទល្មើសនេះ អាចមានព្យសនកម្មខាងផ្លូវចិត្ត ព្យសនកម្មខាងសម្ភារៈ និងព្យសនកម្មដល់សន្តិសុខសណ្តាប់ធ្នាប់សាធារណៈ ។ ឧទាហរណ៍ **លោក ភារម្យ** បានបង្កើតជាមេរោគ ហើយបានវាយប្រហារគេហទំព័ររបស់រាជរដ្ឋាភិបាល ដែលធ្វើឱ្យគេហទំព័រនោះខូចលែងដំណើរការ ។

២.២.៣ ទំនាក់ទំនងហេតុ និងផល

ទាក់ទងនឹងទំនាក់ទំនងហេតុនេះ ប្រសិនបើ **លោក ភារម្យ** មិនបានបង្កើតតំណភ្ជាប់ដែលមានមេរោគទេនោះ ព្យសនកម្មក៏មិនកើតទៅលើ **កញ្ញា សុខា** ដែរ ។

២.៣ ចាត់អត្តនោម័ត

ចំពោះចេតនារបស់ចារីនៃបទល្មើសនេះ យើងសង្កេតឃើញថាចេតនាចម្បងគឺបង្កើតឱ្យមាននូវឧបសគ្គដល់ដំណើរការនៃប្រព័ន្ធប្រព្រឹត្តិកម្មស្ងួយប្រវត្តនៃទិន្នន័យរបស់ជនរងគ្រោះ ។ មានន័យថា ចារីបានចេតនាទុច្ចរិតរួចហើយ ពោលគឺមានចេតនាធ្វើឱ្យខូចដំណើរការប្រព័ន្ធប្រព្រឹត្តិកម្មស្ងួយប្រវត្តនៃទិន្នន័យរបស់ជនរងគ្រោះ ។

កថាខណ្ឌទី ៣ បទបញ្ជូល លុបបំបាត់ ឬកែប្រែដោយទុច្ចរិតនូវទិន្នន័យ

៣.១ ចាត់និត្យានុកូល

បទបញ្ជូល លុបបំបាត់ ឬ កែប្រែដោយទុច្ចរិតនូវទិន្នន័យទៅក្នុងប្រព័ន្ធប្រព្រឹត្តិកម្មស្ងួយប្រវត្តនៃទិន្នន័យ គឺមានចែងនៅក្នុងមាត្រា ៤២៩ នៃក្រមព្រហ្មទណ្ឌកម្ពុជា ឆ្នាំ២០០៩ ។ ក្រមនេះបានចែងថា អំពើបញ្ជូល លុបបំបាត់ ឬ កែប្រែដោយទុច្ចរិតនូវទិន្នន័យទៅក្នុងប្រព័ន្ធប្រព្រឹត្តិកម្មស្ងួយប្រវត្តនៃទិន្នន័យ ត្រូវផ្តន្ទាទោសដាក់ពន្ធនាគារពី ១ (មួយ) ឆ្នាំ ទៅ ២ (ពីរ) ឆ្នាំ និងពិន័យជាប្រាក់ពី ២.០០០.០០០ (ពីរលាន) រៀលទៅ ៤.០០០.០០០ (បួនលាន) រៀល ។[37]

៣.២ ចាត់សត្យានុម័ត

៣.២.១ អំពើ

ជាបឋមទាក់ទងទៅនឹងអំពើរបស់ចារី គឺជាអំពើសកម្ម ហើយធ្វើសកម្មភាពដែលយើងសង្កេតបានថាចារីប្រើប្រាស់ឧបករណ៍អេឡិចត្រនិក ដើម្បីបញ្ជូល ឬ លុបបំបាត់ ឬ កែប្រែនូវទិន្នន័យទៅក្នុងប្រព័ន្ធប្រព្រឹត្តិកម្ម-ស្ងួយប្រវត្តនៃទិន្នន័យ ។ តើអំពើរបស់ចារីក្នុងការបញ្ជូល ឬ លុបបំបាត់ ឬ កែប្រែនូវទិន្នន័យទៅក្នុងប្រព័ន្ធ

[37] ក្រមព្រហ្មទណ្ឌ, លេខ នស/រកម/១២០៧/០៣០, ០៨ ធ្នូ ២០០៩, មាត្រា៤២៩។

ប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យ មានន័យយ៉ាងណា?

- អំពើបញ្ចូលនូវទិន្នន័យទៅក្នុងប្រព័ន្ធប្រព្រឹត្តកម្មស្វ័យប្រវត្តនៃទិន្នន័យ ៖ ទាក់ទងអំពើបញ្ចូលនេះយើងសង្កេតឃើញថាមានច្រើនរូប ។ ម្លោះហើយដើម្បីស្តែងឱ្យឃើញអំពើរបស់ចារីក្នុងសកម្មភាពនៃការបញ្ចូលនូវទិន្នន័យនេះ យើងសូមលើកឧទាហរណ៍ ។ ឧទាហរណ៍ នៅមុនពេលបោះឆ្នោត **លោក សិរី** បានបញ្ចូលអត្តសញ្ញាណអ្នកបោះឆ្នោតដោយគ្មានការអនុញ្ញាតទៅក្នុងគេហទំព័ររបស់គណៈកម្មាធិការជាតិរៀបចំការបោះឆ្នោត ។
- អំពើលុបបំបាត់នូវទិន្នន័យទៅក្នុងប្រព័ន្ធប្រព្រឹត្តកម្មស្វ័យប្រវត្តនៃទិន្នន័យ ៖ មានន័យថា ចារីប្រើប្រាស់ឧបករណ៍អេឡិចត្រូនិកក្នុងការធ្វើសកម្មភាពលុបបំបាត់នូវទិន្នន័យទៅក្នុងប្រព័ន្ធប្រព្រឹត្តកម្មស្វ័យប្រវត្តនៃទិន្នន័យ ឧទាហរណ៍ នៅមុនពេលបោះឆ្នោត **លោក សិរី** បានប្រើប្រាស់កុំព្យូទ័រ ធ្វើសកម្មភាពលុបបំបាត់នូវអត្តសញ្ញាណអ្នកបោះឆ្នោតដោយគ្មានការអនុញ្ញាតទៅក្នុងគេហទំព័ររបស់គណៈកម្មាធិការជាតិរៀបចំការបោះឆ្នោត ។
- អំពើកែប្រែនូវទិន្នន័យទៅក្នុងប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យ ៖ សំដៅទៅលើអំពើដែលចារីប្រើប្រាស់ឧបករណ៍អេឡិចត្រូនិកដើម្បីធ្វើសកម្មភាពកែប្រែទិន្នន័យទៅក្នុងប្រព័ន្ធប្រព្រឹត្តកម្មស្វ័យប្រវត្តនៃទិន្នន័យ ។ ឧទាហរណ៍ **លោក វុត្ថា** បានប្រើប្រាស់កុំព្យូទ័រ ដើម្បីធ្វើសកម្មភាពហែកចូលកុំព្យូទ័ររបស់ **លោក វាសនា** ហើយកែប្រែទិន្នន័យដូចជា ឯកសារ ជាអាទិ៍ ដែលមាននៅក្នុងកុំព្យូទ័ររបស់ **លោក វាសនា** ។

៣.២.២ ព្យសនកម្ម

ដូចជាបទល្មើសមុនៗអញ្ចឹង បទល្មើសនេះអាចបង្កើតឱ្យមានព្យសនកម្មខាងសម្ភារៈ ព្យសនកម្មខាងផ្លូវចិត្ត និងពស្យនកម្មដែលបង្កចលាចលដល់សន្តិសុខសណ្តាប់ធ្នាប់សង្គម ។

៣.២.៣ ទំនាក់ទំនងហេតុ និងផល

តាមឧទាហរណ៍ខាងលើ ប្រសិនបើ **លោក វុត្ថា** មិនធ្វើការហែកចូល ហើយកែប្រែនូវទិន្នន័យទៅក្នុងប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តិនៃទិន្នន័យរបស់ **លោក វាសនា** ទេ នោះក៏មិនកើតមាននូវព្យសនកម្មដល់ **លោក វាសនា** ដែរ ។

៣.៣ ឆាតុអត្តនោម័ត

អត្តនោម័តរបស់ចារីក្នុងការប្រព្រឹត្តបទល្មើសនេះ គឺចារីមានកំហុសចេតនា ពោលគឺចេតនាទុច្ចរិតក្នុងរបស់ចារីក្នុងការបញ្ចូល លុបបំបាត់ ឬ កែប្រែនូវទិន្នន័យទៅក្នុងប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តិនៃទិន្នន័យរបស់ជនរងគ្រោះ ។ បន្ថែមពីនេះ យើងក៏អាចគិតពិចារណាបានថា ជាទូទៅចារីគ្មានឆន្ទៈក្នុងការទទួលបានប្រយោជន៍ពីជនរងគ្រោះនោះទេ មានន័យថាឆន្ទៈចម្បងរបស់ចារី គឺដើម្បីសម្រេចនូវការបញ្ចូល លុបបំបាត់ ឬ កែប្រែនូវទិន្នន័យរបស់ជនរងគ្រោះ ។

កថាខណ្ឌទី ៤ បទចូលរួមក្នុងក្រុមប្រមូលផ្តុំ ឬ ក្នុងសន្និដ្ឋិភាពដើម្បីរៀបចំប្រព្រឹត្តបទល្មើស

មុននឹងធ្វើការបកស្រាយទៅលើកថាខណ្ឌទី១ យើងសូមគូសបញ្ជាក់ថា ជនល្មើសបានប្រមូលផ្តុំជាក្រុមដែលមានការចាត់តាំង ពោលគឺជាការប្រមូលផ្តុំដែលបង្កើតឡើង ឬ ក្នុងសន្និដ្ឋិភាពដើម្បីត្រៀមរៀបចំ ឬ ប្រព្រឹត្តបទល្មើសមួយ ឬ ច្រើន ។[38] គូសបញ្ជាក់ថា នៅក្នុងកថាខណ្ឌទី៤នេះ យើងនឹងមិនបកស្រាយអំពីស្ថានទម្ងន់ទោសនោះទេ ។ ម្លោះហើយ យើងគ្រាន់តែសិក្សាអំពីធាតុផ្សំនៃបទល្មើសនេះតែប៉ុណ្ណោះ ។

៤.១ ធាតុនីត្យានុកូល

បទចូលរួមក្នុងក្រុមប្រមូលផ្តុំ ឬ ក្នុងសន្និដ្ឋិភាពដើម្បីរៀបចំប្រព្រឹត្តបទល្មើស មានចែងនៅក្នុងមាត្រា ៤៣០ នៃក្រមព្រហ្មទណ្ឌកម្ពុជា ឆ្នាំ២០០៩ ។ ក្រមនេះបានបញ្ញត្តថា អំពើចូលរួមទៅក្នុងក្រុមប្រមូលផ្តុំ ឬទៅក្នុងសន្និដ្ឋិភាពដែលបង្កើតឡើងដើម្បីរៀបចំប្រព្រឹត្តបទល្មើសដែលមានចែងក្នុងបទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យា ត្រូវផ្តន្ទាទោសដាក់ពន្ធនាគារពី ១ (មួយ) ឆ្នាំ ទៅ ២ (ពីរ) ឆ្នាំ និងពិន័យជាប្រាក់ពី ២.000.000 (ពីរលាន) រៀល ទៅ ៤.000.000 (បួនលាន) រៀល ។[39]

៤.២ ធាតុសត្យានុម័ត

៤.២.១ អំពើ

បើយើងនិយាយអំពីអំពើរបស់ចារី យើងកត់សម្គាល់ឃើញថាជាអំពើសកម្ម ពោលចារីបានដឹងហើយថាការចូលរួមក្នុងក្រុមប្រមូលផ្តុំ ឬ សន្និដ្ឋិភាពដើម្បីរៀបចំប្រព្រឹត្តបទល្មើស ជាអំពើដែលច្បាប់បានហាមឃាត់ ។ ឧទាហរណ៍ **លោក ដេវីត លោក រិទ្ធ** និងមានគ្នីគ្នាច្រើននាក់ទៀត បានដឹងហើយថាការដែលបង្កើតជាក្រុមប្រមូលផ្តុំ ឬ សន្និដ្ឋិភាព ដើម្បីធ្វើការហែកចូលគេហទំព័រគណៈកម្មាធិការជាតិរៀបចំការបោះឆ្នោត គឺជាបទល្មើស ។ បើទោះបីជា **លោក ដេវីត លោក រិទ្ធ** និងគ្នីគ្នា បានដឹងរួចហើយក៏ដោយក៏ **លោក ដាវីត លោក រិទ្ធ** និងគ្នីគ្នា នៅតែបង្កើតជាក្រុមប្រមូលផ្តុំដើម្បីរៀបចំប្រព្រឹត្តបទល្មើស ដដែរ ។

៤.២.២ ព្យសនកម្ម

យើងឃើញថា ចារីបានចូលរួមទៅក្នុងការប្រមូលផ្តុំ ឬទៅក្នុងសន្និដ្ឋិភាព ដើម្បីរៀបចំប្រព្រឹត្តបទល្មើស ។

តាមការសិក្សាស្រាវជ្រាវ ជាគោលការណ៍ត្រឹមតែការគិត និងរៀបចំមិនទាន់កើតមានបទល្មើសនោះទេ ទាល់តែចារីចាប់ផ្តើមប្រព្រឹត្ត ឬ ចារីប្រព្រឹត្តបទល្មើសបានសម្រេច ឬ បំពេញលក្ខខណ្ឌនៃការប៉ុនប៉ង នោះទើបកើតមានបទល្មើស ហើយព្យសនកម្មនឹងកើតមានឡើង ។

ដោយឡែក យើងពិនិត្យឃើញថា បទចូលរួមក្នុងក្រុមប្រមូលផ្តុំ ឬ ក្នុងសន្និដ្ឋិភាពដើម្បីរៀបចំប្រព្រឹត្ត

[38]ក្រមព្រហ្មទណ្ឌ, លេខ នស/រកម/១២០៧/០៣០, ០៨ ធ្នូ ២០០៩, មាត្រា៧៧។

[39]ក្រមព្រហ្មទណ្ឌ, លេខ នស/រកម/១២០៧/០៣០, ០៨ ធ្នូ ២០០៩, មាត្រា៤៣០។

បទល្មើសនេះ មិនទាន់កើតមានព្យសនកម្មនោះទេ ។ តាមទស្សនៈផ្ទាល់ខ្លួន នីតិករយល់ឃើញថាប្រសិនបើមិនបានបញ្ញត្តបែបនេះទេនោះ ព្យសនកម្មនឹងអាចកើតមានក្នុងវិសាលភាពធំដែលមិនអាចព្យៀងទុកជាមុនបាននាថ្ងៃអនាគត ។ ឧទាហរណ៍ ក្រុមហែកគ័រមួយក្រុមបានត្រៀមរៀបចំហែកចូលគេហទំព័រគណៈកម្មាធិការជាតិរៀបចំការបោះឆ្នោត នៅអំឡុងពេលបោះឆ្នោតខាងមុខនេះ ។ ម្ល៉ោះហើយ ប្រសិនបើមិនមានការបញ្ញត្តិទុកជាមុនទេ ព្យសនកម្មនោះនឹងបង្កឱ្យមានភាពចលាចល អសន្តិសុខសណ្តាប់ធ្នាប់សាធារណៈជាក់ជាពុំខាន ។

៤.២.៣ ឆាតុអត្តឆោម័ត

ទាក់ទងនឹងចេតនារបស់ចារី គឺចារីមានចេតនាក្នុងការចូលរួមទៅក្នុងក្រុមប្រមូលផ្តុំ ឬទៅក្នុងសន្និដ្ឋិភាពដើម្បីរៀបចំប្រព្រឹត្តបទល្មើស ។ មានន័យថា ចេតនារបស់ចារី គឺគ្រោងនឹងប្រព្រឹត្តបទល្មើសនៅថ្ងៃអនាគត ។

ចំណុចដែលយើងគួរកត់សម្គាល់៖ គឺនៅត្រង់ទោសដាក់ពន្ធនាគារ និងទោសពិន័យជាប្រាក់ដែលបានបកស្រាយនៅក្នុងផ្នែកនេះ គឺជាបទមជ្ឈិមដូចគ្នា ពោលចាប់ពីមាត្រា៤២៧ ដល់ មាត្រា៤៣០ ទោសដាក់ពន្ធនាគារគឺចាប់ពី ១ (មួយ) ឆ្នាំ ទៅដល់ ២ (ពីរ) ឆ្នាំ និងពិន័យជាប្រាក់ពី ២.000.000 (ពីរ) លានរៀល ដល់ ៤.000.000 (បួនលាន) រៀល លើកលែងតែកថាខណ្ឌទី១ នៃមាត្រា៤២៧ ។

កថាខណ្ឌទី ៥ ការប៉ុនប៉ង

ក្នុងករណីដែលច្បាប់បានចែងទុកក្នុងបទមជ្ឈិម អាចត្រូវផ្តន្ទាទោសបាន កាលណាលក្ខខណ្ឌខាងក្រោមនេះត្រូវបានបំពេញ៖

- ចារីបានចាប់ផ្តើមអនុវត្តបទល្មើស មានន័យថា ចារីបានប្រព្រឹត្តបទល្មើសដែលមានគោលបំណងដោយផ្ទាល់ដើម្បីប្រព្រឹត្តបទល្មើស និង
- ចារីមិនបានបញ្ឈប់អំពើរបស់ខ្លួនទៅវិញដោយស្ម័គ្រចិត្ត តែត្រូវបានរាំងស្ទះ ឬ អាក់ខានដោយឥទ្ធិពលនៃកាលៈទេសៈក្រៅឆន្ទៈរបស់ខ្លួន ។[40]

ចំពោះបទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យា ការប៉ុនប៉ងប្រព្រឹត្តបទមជ្ឈិមដែលមានចែងក្នុងបទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យា ត្រូវផ្តន្ទាទោសដូចគ្នានឹងបទមជ្ឈិមខាងលើ ។[41] មានន័យថា ក្នុងករណីដែលចារីបានបំពេញនូវលក្ខខណ្ឌនៃការប៉ុនប៉ង នោះចារីនឹងត្រូវផ្តន្ទាទោសដូចគ្នានឹងបទមជ្ឈិម ។

កថាខណ្ឌទី ៦ ទោសបន្ថែម

ទោសបន្ថែម គឺជាទោសដែលបន្ថែមទៅលើមូលទោស ។ បទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យានេះ ក៏មានចែងអំពីទោសបន្ថែមផងដែរ ។ ចំពោះបទមជ្ឈិមដែលមានចែងអំពីបទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យានេះ

[40]ក្រមព្រហ្មទណ្ឌ, លេខ នស/រកម/១២០៧/០៣០, ០៨ ធ្នូ ២០០៩, មាត្រា២៧។

[41]ក្រមព្រហ្មទណ្ឌ, លេខ នស/រកម/១២០៧/០៣០, ០៨ ធ្នូ ២០០៩, មាត្រា៤៣១។

ទោសបន្ថែមមានដូចតទៅ អាចត្រូវបានប្រកាស៖[42]

១-ការដកសិទ្ធិខ្លះជាពលរដ្ឋ ជាស្ថាពរ ឬ សម្រាប់រយៈពេល ៥ (ប្រាំ) ឆ្នាំ យ៉ាងច្រើន ។

២-ការហាមឃាត់ចំពោះការប្រកបវិជ្ជាជីវៈ កាលបើបទល្មើសនេះបានប្រព្រឹត្តនៅក្នុងការប្រកបវិជ្ជាជីវៈ ឬ នៅក្នុងឱកាសនៃការប្រកបវិជ្ជានេះជាស្ថាពរ ឬ សម្រាប់រយៈពេល ៥ (ប្រាំ) ឆ្នាំ យ៉ាងច្រើន ។

៣-ការរឹបអូសឧបករណ៍ សម្ភារៈ ឬ វត្ថុណាមួយ ដែលប្រើប្រាស់សម្រាប់ប្រព្រឹត្តបទល្មើស ឬ ដែលមានគោលដៅប្រព្រឹត្តបទល្មើស ។

៤-ការរឹបអូសវត្ថុ ឬ មូលនិធិ ដែលជាកម្មវត្ថុនៃបទល្មើស ។

៥-ការរឹបអូសផលទុន និងទ្រព្យសម្បត្តិដែលជាផលកើតចេញពីបទល្មើស ។

៦-ការរឹបអូសឧបភោគភណ្ឌ សម្ភារៈ ឬ ចលនវត្ថុនៅក្នុងកន្លែងដែលបទល្មើសនោះបានប្រព្រឹត្ត ។

៧-ការរឹបអូសយានជំនិះរបស់ទណ្ឌិតមួយគ្រឿង ឬ ច្រើនគ្រឿង ។

៨-ការបិទផ្សាយសេចក្តីសម្រេចផ្តន្ទាទោសសម្រាប់រយៈពេល ២ (ពីរ) ខែ យ៉ាងច្រើន ។

៩-ការផ្សាយសេចក្តីសម្រេចផ្តន្ទាទោសនៅក្នុងសារព័ត៌មាន ។

១០-ការផ្សាយសេចក្តីសម្រេចផ្តន្ទាទោស តាមគ្រប់មធ្យោបាយទូរគមនាគមន៍សោតទស្សន៍ សម្រាប់រយៈពេល ៨ (ប្រាំបី) ថ្ងៃ យ៉ាងច្រើន ។

ផ្នែកទី ២ ស្ថាប័នជំនាញ

នៅកម្ពុជាយើងសម័យឌីជីថល ជាទូទៅពឹងផ្អែកលើបច្ចេកវិទ្យាដើម្បីអភិវឌ្ឍប្រទេស ។ ក៏ប៉ុន្តែតម្រូវការនេះបានបង្កឱ្យមានបទល្មើសបច្ចេកវិទ្យាមិនតិចទេ ។ យ៉ាងណាក្តី នាសម័យឌីជីថល កម្ពុជាបានបង្កើតស្ថាប័នជំនាញមួយចំនួនដែលមានតួនាទីចម្បង ក្នុងការការពារ បង្ការ បង្ក្រាប ឆ្លើយតប និងផ្សព្វផ្សាយជាដើម ។ សូមបញ្ជាក់ថា បទល្មើសព័ត៌មានវិទ្យា ទាមទារឱ្យមានស្ថាប័នដែលមានជំនាញ ធនធានមនុស្ស ធនធានហិរញ្ញវត្ថុ ជាអាទិ៍ ដែលមានភាពច្បាស់លាស់ទាក់ទងនឹងបច្ចេកវិទ្យា ។ គួរបញ្ជាក់ថា នៅក្នុងផ្នែកនេះយើងមិនលើកយកស្ថាប័នជំនាញទាំងអស់មកសិក្សានោះទេ ពោលគឺយើងសង្កេតឃើញស្ថាប័នជំនាញពីរដែលសំខាន់ គឺ **នាយកដ្ឋានប្រឆាំងបទល្មើសបច្ចេកវិទ្យា**(កថាខណ្ឌទី១) និង**ការិយាល័យឆ្លើយតបបញ្ហាបន្ទាន់នៃកុំព្យូទ័រ** (កថាខណ្ឌទី ២) ។

កថាខណ្ឌទី ១ នាយកដ្ឋានប្រឆាំងនឹងបទល្មើសបច្ចេកវិទ្យា

នាយកដ្ឋានប្រឆាំងបទល្មើសបច្ចេកវិទ្យាត្រូវបានបង្កើតឡើងតាមរយៈអនុក្រឹត្យលេខ១០៩ ស្តីពីការ

[42]ក្រមព្រហ្មទណ្ឌ, លេខ នស/រកម/១២០៧/០៣០, ០៨ ធ្នូ ២០០៩, មាត្រា៤៣២។

រៀបចំ និងការប្រព្រឹត្តទៅនៃក្រសួងមហាផ្ទៃ ចុះថ្ងៃទី ១៩ ខែសីហា ឆ្នាំ ២០១៥ ។ ក្រសួងមហាផ្ទៃបានសម្រេចបង្កើតនាយកដ្ឋានប្រឆាំងនឹងបទល្មើសបច្ចេកវិទ្យា ដើម្បីស៊ើបអង្កេត និងបង្ក្រាបបទល្មើសនានានៅលើប្រព័ន្ធអ៊ីនធឺណិត ជាអាទិ៍ ។ ទៀតនោះ ក៏សំដៅចាត់វិធានការចំពោះសកម្មភាពដែលក្រសួងចាត់ទុកថា ជាការញុះញង់ ជេរប្រមាថ និងរើសអើងពូជសាសន៍តាមប្រព័ន្ធអ៊ីនធឺណិតផងដែរ ។ ល្អឹកនេះ ចំណុចសំខាន់ដែលយើងនឹងសិក្សាបន្ថែមទៀតនោះ **រចនាសម្ព័ន្ធនាយកដ្ឋានប្រឆាំងបទល្មើសបច្ចេកវិទ្យា**(កថាខណ្ឌទី១) និង**ភារកិច្ចរបស់នាយកដ្ឋានប្រឆាំងបទល្មើស**(កថាខណ្ឌទី២) និង**ការដាក់ពាក្យបណ្តឹង**(កថាខណ្ឌទី៣) ។

១.១ រចនាសម្ព័ន្ធនាយកដ្ឋានប្រឆាំងនឹងបទល្មើសបច្ចេកវិទ្យា

យោងតាម អនុក្រឹត្យលេខ ១០៩ ស្តីពីការរៀបចំ និងការប្រព្រឹត្តទៅនៃក្រសួងមហាផ្ទៃ នាយកដ្ឋានប្រឆាំងនឹងបទល្មើសបច្ចេកវិទ្យា គឺជាសេនាធិការឱ្យអគ្គស្នងការដ្ឋាននគរបាលជាតិ នៃក្រសួងមហាផ្ទៃ ។[43] នាយកដ្ឋានប្រឆាំងនឹងបទល្មើសបច្ចេកវិទ្យាមានសមាសភាព ប្រធាន អនុប្រធានតាមការកំណត់ និងសមាជិកជាច្រើនរូប ។[44]

១.២ ភារកិច្ចរបស់នាយកដ្ឋានប្រឆាំងបទល្មើសបច្ចេកវិទ្យា

អនុក្រឹត្យនេះ បានចែងថា នាយកដ្ឋានប្រឆាំងបទល្មើសបច្ចេកវិទ្យា មានតួនាទីធ្វើជាសេនាធិការក្នុងការសិក្សារៀបចំគោលការណ៍ គោលនយោបាយ យុទ្ធសាស្ត្រ ផែនការសកម្មភាពលើការងារបង្ការ ទប់ស្កាត់ សំដៅរួមចំណែកការពារ សន្តិសុខជាតិ រក្សាសណ្តាប់ធ្នាប់សាធារណៈ សុវត្ថិភាពសង្គមដែលមានភារកិច្ចដូចខាងក្រោម៖[45]

- សិក្សារៀបចំគោលការណ៍ វិធានការ យុទ្ធសាស្ត្រ និងផែនការសកម្មភាពលើការបង្ការ ទប់ស្កាត់ ស្រាវជ្រាវ ស៊ើបអង្កេត និងបង្ក្រាបបទល្មើសបច្ចេកវិទ្យា
- សហការជាមួយបណ្តាស្ថាប័នរដ្ឋ និងឯកជនដែលផ្តត់ផ្តង់សេវាបច្ចេកវិទ្យា និងទូរគមនាគមន៍គ្រប់ប្រភេទដើម្បីគ្រប់គ្រងលិខិតបង្ហានជួល ជាវសេវាទូរគមនាគមន៍បម្រើឱ្យការស្រាវជ្រាវ ស៊ើបអង្កេត ប្រមូលភស្តុតាង និងបង្ក្រាបបទល្មើសបទល្មើសបច្ចេកវិទ្យា
- សហការជាមួយបណ្តាស្ថាប័នរដ្ឋ និងឯកជនដែលពាក់ព័ន្ធដើម្បីផ្លាស់ប្តូរបទពិសោធន៍ និងការងារបណ្តុះបណ្តាលដើម្បីលើកកម្ពស់សមត្ថភាពចំណេះដឹងលើកិច្ចប្រតិបត្តិការ ប្រយុទ្ធប្រឆាំងបទល្មើសបច្ចេកវិទ្យា
- ប្រមូល និងវិភាគទិន្នន័យប្រព័ន្ធទូរគមនាគមន៍ សំដៅរកឱ្យឃើញបទល្មើស និងការគំរាមកំហែងដល់

[43]អនុក្រឹត្យស្តីពីការរៀបចំ និងការប្រព្រឹត្តទៅនៃក្រសួងមហាផ្ទៃ, ១០៩, ១៩ សីហា ២០១៥, កថាខណ្ឌទី២ ចំណុចទី៥.៦ នៃមាត្រា២៩។
[44]អនុក្រឹត្យស្តីពីការរៀបចំ និងការប្រព្រឹត្តទៅនៃក្រសួងមហាផ្ទៃ, ១០៩, ១៩ សីហា ២០១៥, កថាខណ្ឌទី១ ចំណុចទី៥.៦ នៃមាត្រា២៩។
[45]អនុក្រឹត្យស្តីពីការរៀបចំ និងការប្រព្រឹត្តទៅនៃក្រសួងមហាផ្ទៃ, ១០៩, ១៩ សីហា ២០១៥, ចំណុចទី៥.៦ នៃមាត្រា២៩។

សន្តិសុខជាតិ ដើម្បីចាត់វិធានការតាមច្បាប់

- ស៊ើបអង្កេត និងចាត់វិធានការតាមច្បាប់ចំពោះសកម្មភាពញុះញង់ ជេរប្រមាថ ពីសអើងពូជសាសន៍ បង្កចលាចលក្នុងសង្គម តាមប្រព័ន្ធអ៊ីនធឺណិត
- ស្រាវជ្រាវ ស៊ើបអង្កេត និងបង្ក្រាបការជ្រៀតជ្រែកចូល និងបំផ្លិចបំផ្លាញប្រព័ន្ធព័ត៌មានវិទ្យា ការបង្កើតមេរោគកុំព្យូទ័របំផ្លាញឯកសារ ឬ បង្កការរំខានដល់ដំណើរការប្រព័ន្ធបច្ចេកវិទ្យា និងការធ្វើចារកម្មទិន្នន័យ
- ស្រាវជ្រាវស៊ើបអង្កេត និងបង្ក្រាបការបើកល្បែងស៊ីសងខុសច្បាប់ តាមប្រព័ន្ធអ៊ីនធឺណិត នៅក្នុងព្រះរាជាណាចក្រកម្ពុជា
- ស្រាវជ្រាវស៊ើបអង្កេត និងបង្ក្រាបបទល្មើសក្លែងបន្លំលួចប្រាក់តាមប្រព័ន្ធធនាគារ
- ស្រាវជ្រាវធ្វើកោសលវិច័យ និងវិភាគទិន្នន័យក្នុងឧបករណ៍បច្ចេកទេស សំដៅរកឃើញភស្តុតាងសម្រាប់បម្រើផ្លូវច្បាប់
- សហការផ្តល់ជំនួយផ្នែកបច្ចេកទេសកោសលវិច័យដល់ស្ថាប័ន ដែលមានសមត្ថកិច្ចពាក់ព័ន្ធសម្រាប់បម្រើនីតិវិធីច្បាប់
- សហប្រតិបត្តិការជាមួយស្ថាប័នជាតិ និងអន្តរជាតិដែលពាក់ព័ន្ធដើម្បីផ្លាស់ប្តូរព័ត៌មានចារកម្មសំដៅមានវិធានការទាន់ពេលវេលា
- ធ្វើការងាររដ្ឋបាល បុគ្គលិក បណ្តុះបណ្តាល និងការងារភស្តុតាង គណនេយ្យរបស់នាយកដ្ឋាន
- ធ្វើរបាយការណ៍បូកសរុបលទ្ធផលការងារ និងទិសដៅរបស់នាយដ្ឋានប្រឆាំងបទល្មើសបច្ចេកវិទ្យាតាមកំណត់
- ទទួលអនុវត្តភារកិច្ច និងសិទ្ធិផ្សេងៗទៀតដែលប្រធាននាយកដ្ឋានកណ្តាលសន្តិសុខប្រគល់ឱ្យ នាយកដ្ឋានប្រឆាំងនឹងបទល្មើសបច្ចេកវិទ្យា ដឹកនាំដោយប្រធានមួយរូប និងមានអនុប្រធានមួយចំនួនតាមការកំណត់ ។

១.៣ ការដាក់ពាក្យបណ្តឹង

ក្នុងករណីដែលអ្នកប្រើប្រាស់ បណ្តាញសង្គម ឬ ប្រព័ន្ធបច្ចេកវិទ្យា មានបញ្ហាដែលអាចកើតឡើងពីបទល្មើសបច្ចេកវិទ្យា នោះអ្នកប្រើប្រាស់អាចដាក់ពាក្យបណ្តឹងទៅកាន់ នាយកដ្ឋានប្រឆាំងនឹងបទល្មើសបច្ចេកវិទ្យាបាន ។ ការដាក់ពាក្យបណ្តឹងពាក់ព័ន្ធនឹងបទល្មើសបច្ចេកវិទ្យា គឺអាចដាក់ពាក្យបណ្តឹងបានទាំងនៅនាយកដ្ឋានផ្ទាល់ក៏បាន ឬ ក៏អាចដាក់ពាក្យបណ្តឹងតាមអនឡាញក៏បានដែរ ។ ទាក់ទងនឹងការដាក់ពាក្យបណ្តឹងនៅនាយកដ្ឋានផ្ទាល់ ដែលនាយកដ្ឋានប្រឆាំងនឹងបទល្មើសបច្ចេកវិទ្យាមានទីតាំងស្ថិតនៅអគារ*អ៊ិល* (L) នៃក្រសួង

មហាផ្ទៃ មហាវិថីព្រះនរោត្តម រាជធានីភ្នំពេញ ។ ដោយសារតែការដាក់ពាក្យបណ្តឹងទៅកាន់នាយកដ្ឋានដោយផ្ទាល់ និងការដាក់ពាក្យបណ្តឹងទៅនាយកដ្ឋានតាមប្រព័ន្ធអនឡាញ ត្រូវភ្ជាប់មកនូវឯកសារដូចគ្នា ។ ល្អីកនេះយើងសូមលើកនូវករណីការដាក់ពាក្យបណ្តឹងតាមប្រព័ន្ធអនឡាញ មូលហេតុដោយសារការរីករាលដាលនៃជម្ងឺកូវីដ-១៩ ព្រមទាំងយោងតាមវិធានការណ៍របស់ក្រសួងសុខាភិបាល ក្នុងការទប់ស្កាត់ការឆ្លងកូវីដ-១៩ ជាដើម ។

ក្នុងករណីដែលអ្នកប្រើប្រាស់បណ្តាញសង្គម ឬ ប្រព័ន្ធបច្ចេកវិទ្យា ត្រូវបានរងគ្រោះដោយបទល្មើសព័ត៌មានវិទ្យា ឬ ការបោកបញ្ឆោតតាមរយៈអនឡាញ មានដូចជា ការលួចចូល លុប ឬ យកនូវគណនីបណ្តាញសង្គម ជាអាទិ៍ ។ អ្នកប្រើប្រាស់បណ្តាញសង្គម ឬ ប្រព័ន្ធបច្ចេកវិទ្យា អាចដាក់ពាក្យបណ្តឹងតាមវិធីដូចខាងក្រោម៖[46]

១-សូមបំពេញពាក្យបណ្តឹងដែលមាននៅក្នុងឧបសម្ព័ន្ធ

២-ភ្ជាប់មកជាមួយនូវ អត្តសញ្ញាណប័ណ្ណ ឬ សំបុត្រកំណើត ឬ លិខិតឆ្លងដែន និងសូមថតរូបផ្ទាល់ខ្លួនជាមួយឯកសារនេះ

៣-សូមភ្ជាប់មកនូវរូបភាពស្ក្រីនស៊ីតទាក់ទងនឹងបទល្មើសព័ត៌មានវិទ្យា ឬ ការបោកបញ្ឆោត ។

បន្ទាប់ពីអ្នកប្រើប្រាស់បណ្តាញសង្គម ឬ ប្រព័ន្ធបច្ចេកវិទ្យា ដែលរងគ្រោះ បានប្រមូលឯកសារទាំងបីខាងលើនេះ អ្នកប្រើប្រាស់បណ្តាញសង្គម ឬ ប្រព័ន្ធបច្ចេកវិទ្យា ដែលរងគ្រោះអាចធ្វើមកនាយកដ្ឋានតាមរយៈមីសសេនជរ @anti.cyber.crime.department ឬ តាមរយៈអ៊ីម៉ែល accd.police@cyber.police.gov.kh ។ ប្រសិនបើអ្នកប្រើប្រាស់បណ្តាញសង្គម ឬ ប្រព័ន្ធបច្ចេកវិទ្យា ដែលរងគ្រោះ ត្រូវការរកជំនួយក្នុងការដាក់ពាក្យបណ្តឹង អាចទាក់ទងមកនាយកដ្ឋានតាមទូរស័ព្ទលេខ ០២៣ ៧២៦ ៨២២ រៀងរាល់ម៉ោងធ្វើការ ។

កថាខណ្ឌទី ២ ការិយាល័យឆ្លើយតបបញ្ជាបន្ទាន់នៃកុំព្យូទ័រ

ការិយាល័យឆ្លើយតបបញ្ជាបន្ទាន់នៃកុំព្យូទ័រ(CamCERT) គឺជាការិយាល័យបង្គោលនៅកម្ពុជាសម្រាប់ទំនាក់ទំនងបញ្ជាពាក់ព័ន្ធទៅនឹងសន្តិសុខតាមអ៊ីនធឺណិត និងបច្ចេកវិទ្យាដែលមានផលវិបាកដល់អ្នកប្រើប្រាស់អ៊ីនធឺណិតនៅកម្ពុជា ។[47] នៅក្នុងកថាខណ្ឌទី២ យើងនឹងសិក្សាអំពី**រចនាសម្ព័ន្ធនៃការិយាល័យឆ្លើយតបបញ្ជាបន្ទាន់នៃកុំព្យូទ័រ**(២.១) និង**ភារកិច្ច**(២.៣) ។

២.១ រចនាសម្ព័ន្ធនៃការិយាល័យឆ្លើយតបបញ្ជាបន្ទាន់នៃកុំព្យូទ័រ

ការិយាល័យនេះ ស្ថិតនៅក្រោមនាយកដ្ឋានសន្តិសុខបច្ចេកវិទ្យាគមនាគមន៍ និងព័ត៌មាន នៃ

[46] នាយកដ្ឋានប្រឆាំងនឹងបទល្មើសបច្ចេកវិទ្យា (ចូលទស្សនានៅថ្ងៃទី១១ ខែមិថុនា ឆ្នាំ២០២១)។

[47] https://www.camcert.gov.kh/who-we-are/ (ចូលទស្សនានៅថ្ងៃទី១១ ខែមិថុនា ឆ្នាំ២០២១)។

អគ្គនាយកដ្ឋានបច្ចេកវិទ្យាគមនាគមន៍ និងព័ត៌មាន នៃក្រសួងប្រៃសណីយ៍ និងទូរគមនាគមន៍ ។[48] ទៀតសោត នោះ ការិយាល័យឆ្លើយតបបញ្ហាបន្ទាន់នៃកុំព្យូទ័រមានចក្ខុវិស័យ ក្នុងការបង្កើនទំនុកចិត្ត និងសន្តិសុខក្នុងការប្រើប្រាស់បច្ចេកវិទ្យាគមនាគមន៍និងព័ត៌មាននៅក្នុងព្រះរាជាណាចក្រកម្ពុជា និងមានបេសកម្មក្នុងការបង្កើនសន្តិសុខអ៊ីនធឺណិតឲ្យបានខ្ពស់បំផុតនៅក្នុងប្រទេស ។[49]

២.២ តារាកិច្ច

ការិយាល័យឆ្លើយតបបញ្ហាបន្ទាន់នៃកុំព្យូទ័រ មានភារកិច្ច៖[50]

- សិក្សា ស្រាវជ្រាវ និងចងក្រងឯកសារស្តីពីការវាយប្រហារមកលើហេដ្ឋារចនាសម្ព័ន្ធព័ត៌មានជាតិ និងម៉ាស៊ីនមេរបស់រាជរដ្ឋាភិបាល
- រៀបចំប្រព័ន្ធជូនដំណឹងជាមុនស្តីអំពីសន្តិសុខព័ត៌មាន
- គ្រប់គ្រងនិងធ្វើបច្ចុប្បន្នភាពគេហទំព័រ និងសារអេឡិចត្រូនិចរបស់ការិយាល័យ CamCERT
- ត្រួតពិនិត្យចរាចរទិន្នន័យ ដែលវាយប្រហារមកលើម៉ាស៊ីនមេរបស់រាជរដ្ឋាភិបាល និងវិស័យឯកជន
- សិក្សា ស្រាវជ្រាវបច្ចេកវិទ្យាថ្មីៗដើម្បីបង្កើនសន្តិសុខបច្ចេកវិទ្យាគមនាគមន៍ និងព័ត៌មាន
- សហប្រតិបត្តិការជាមួយក្រុមការងារសន្តិសុខបច្ចេកវិទ្យាគមនាគមន៍ និងព័ត៌មានផ្សេងៗនៅក្នុងតំបន់ និងពិភពលោក
- គ្រប់គ្រងមជ្ឈមណ្ឌលជាតិទទួលបន្ទុកការងារសន្តិសុខបច្ចេកវិទ្យាគមនាគមន៍ និងព័ត៌មាន

ក្នុងករណីមានបញ្ហាបន្ទាន់នៃកម្មវិធីកុំព្យូទ័រ អ្នកអាចរាយការណ៍ឧប្បទេវហេតុនៃបញ្ហាទាំងនោះតាមអ៊ីម៉ែល incident@camcert.gov.kh ហើយការិយាល័យនេះមានអាស័យដ្ឋាន ផ្ទះលេខ១៣ មហាវិថីព្រះមុន្នីវង្ស រាជធានីភ្នំពេញ រៀងរាល់ម៉ោងធ្វើការ និងមានលេខទូរស័ព្ទ:០២៣ ៧២២ ៣៩១ ។

[48] https://www.camcert.gov.kh/who-we-are/ (ចូលទស្សនានៅថ្ងៃទី១១ ខែមិថុនា ឆ្នាំ២០២១)។

[49] https://www.camcert.gov.kh/who-we-are/ (ចូលទស្សនានៅថ្ងៃទី ១០ ខែឧសភា ឆ្នាំ២០២១)។

[50] ប្រកាសស្តីពីការរៀបចំ និងការប្រព្រឹត្តទៅរបស់នាយកដ្ឋាន និងអង្គភាពក្រោមឱវាទអគ្គនាយកដ្ឋានបច្ចេកវិទ្យាគមនាគមន៍ និងព័ត៌មាន, លេខ ១២៥ បទ. ប្រក, ០២ មិថុនា ២០១៤, ប្រការ៤០។

ជំពូកទី ៣
យុទ្ធសាស្ត្រឈ្នះឈ្នះប្រឆាំងនឹងបទល្មើសព័ត៌មានវិទ្យានៅកម្ពុជា

គេព្យាករណ៍ថានៅឆ្នាំ២០២១នេះ ការខូចខាតដែលកើតឡើងពីបទល្មើសព័ត៌មានវិទ្យានៅលើពិភពលោកមានតម្លៃរហូតដល់ **៦០.០០០.០០០.០០០ (ហុសសិបពាន់) លានដុល្លារ** ហើយរៀងរាល់ **១៦ (ដប់ប្រាំមួយ) វិនាទី** ម្តងគឺមានការវាយប្រហារតាមប្រព័ន្ធបច្ចេកវិទ្យាម្តង ។[51] ជាទូទៅបទល្មើសព័ត៌មានវិទ្យា យើងសង្កេតឃើញកើតមានទៅលើកុំព្យូទ័រ ទូរស័ព្ទ និងបណ្តាញសង្គម ដែលជាមុខព្រួញនៃការវាយប្រហាររបស់ចោរបច្ចេកវិទ្យា ។ ដើម្បីអាចទប់ស្កាត់ព្យសនកម្មដែលកើតឡើងបែបនេះ យើងមានយុទ្ធសាស្ត្រឈ្នះឈ្នះចំនួន ២(ពីរ) គឺ **យុទ្ធសាស្ត្រឈ្នះឈ្នះសម្រាប់អ្នកប្រើប្រាស់កុំព្យូទ័រ និងទូរស័ព្ទ**(ផ្នែកទី១) និង**យុទ្ធសាស្ត្រឈ្នះឈ្នះសម្រាប់អ្នកប្រើប្រាស់បណ្តាញសង្គម**(ផ្នែកទី២) ។

ផ្នែកទី ១ យុទ្ធសាស្ត្រឈ្នះឈ្នះសម្រាប់អ្នកប្រើប្រាស់កុំព្យូទ័រ និងទូរស័ព្ទ

កុំព្យូទ័រ និងទូរស័ព្ទ គឺជាឧបករណ៍ដែលមិនអាចខ្វះបាននៅក្នុងសម័យបច្ចេកវិទ្យា នៅកន្លែងធ្វើការទំនាក់ទំនងគ្នា ជាពិសេសនៅអំឡុងពេលកូវីដ-១៩ នេះ ។ ដ្បិតមានភាពផលវិជ្ជមានបែបនេះក្តី កុំព្យូទ័រ និងទូរស័ព្ទ ក៏ជាផ្នែកមួយដែលបង្កឱ្យអ្នកប្រើប្រាស់ជួបនូវហានិភ័យដែលកើតឡើងពីចោរបច្ចេកវិទ្យា ។ នៅកម្ពុជាយើង អ្នកប្រើប្រាស់មិនតិចទេដែលមិនដឹងអំពីយុទ្ធសាស្ត្រសម្រាប់ការពារកុំព្យូទ័រ និងទូរស័ព្ទ របស់ខ្លួន ។ ប្រសិនបើអ្នកមិនទាន់ដឹងអំពីយុទ្ធសាស្ត្រការពារកុំព្យូទ័រ និងទូរស័ព្ទ សូមកុំបារម្ភណ៍ ។ យើងនឹងលើកយុទ្ធសាស្ត្រឈ្នះឈ្នះប្រឆាំងនឹងបទល្មើសព័ត៌មានវិទ្យាសម្រាប់អ្នកប្រើប្រាស់**កុំព្យូទ័រ**(កថាខណ្ឌទី១) និង**ទូរស័ព្ទ**(កថាខណ្ឌទី២) ។

កថាខណ្ឌទី ១ កុំព្យូទ័រ

កុំព្យូទ័រ គឺជាឧបករណ៍អេឡិចត្រូនិចដែលអាចធ្វើការបានច្រើនយ៉ាង ។ កុំព្យូទ័រទទួលយកទិន្នន័យដែលបានបញ្ចូល ហើយធ្វើការគណនាតាមកម្មវិធីរបស់វា ព្រមទាំងរក្សាទុកនូវទិន្នន័យ ។ នៅរៀងរាល់ ៦ (ប្រាំមួយ) វិនាទីម្តង កុំព្យូទ័រផ្ទាល់ខ្លួនមួយគ្រឿងត្រូវបានគេហែកចូល ។ ជាការពិតណាស់៨០(ប៉ែតសិប) ភាគរយ នៃកុំព្យូទ័របានត្រូវគេហែក ។ ដោយសារតែការវាយប្រហារ កំពុងតែមានការកើនឡើងជាលំដាប់នោះ វាគឺជាការចាំបាច់ណាស់ក្នុងការការពារខ្លួនជៀសវាងក្លាយជាជនរងគ្រោះនៃការប្រើប្រាស់កុំព្យូទ័រ ។ ដើម្បីប្រឆាំងនឹងបទល្មើសព័ត៌មានវិទ្យាទៅលើកុំព្យូទ័ររបស់អ្នក គប្បីអនុវត្តយុទ្ធសាស្ត្រឈ្នះឈ្នះការពារកុំព្យូទ័រ

[51] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (ចូលទស្សនានៅថ្ងៃទី ១០ ខែឧសភា ឆ្នាំ ២០២១)។

ខាងក្រោម៖[52]

- ជៀសវាងការប្រើប្រាស់កុំព្យូទ័រនៅទីតាំងសាធារណៈ
- ជៀសវាងប្រើប្រាស់ វាយហ្វាយ (Wifi) ដែលមិនស្គាល់
- ត្រូវប្រយ័ត្នបំផុតនៅពេលបើកឯកសារភ្ជាប់របស់អ៊ីម៉ែល
- ចូរយកកុំព្យូទ័ររបស់អ្នកទៅជួសជុលតែនៅជាមួយក្រុមហ៊ុនដែលមានកេរ្តិ៍ឈ្មោះល្អ
- ត្រូវបើកដំណើរការមុខងារស្វែងរក (Virus always on) នៃកម្មវិធីកម្ចាត់មេរោគ(Virus) របស់អ្នកជានិច្ច
- ប្រើប្រាស់កម្មវិធីដែលមានអាជ្ញាបណ្ណត្រឹមត្រូវ(Licence Software) ដោយជៀសវាងទាញកម្មវិធីតាមអ៊ីនធឺណិតដែលគ្មានប្រភពច្បាស់លាស់
- ធ្វើបច្ចុប្បន្នភាពប្រព័ន្ធប្រតិបត្តិការ(Operating System) និងកម្មវិធីទាំងអស់ដែលអ្នកមាននៅក្នុងកុំព្យូទ័រឧបករណ៍ចល័តរបស់អ្នកឱ្យបានទៀងទាត់
- ដំឡើងកម្មវិធីកំចាត់ និងទប់ស្កាត់មេរោគ(Anti virus) ហើយធ្វើបច្ចុប្បន្នភាពឱ្យបានជាប្រចាំ
- មិនត្រូវចុចទៅលើតំណភ្ជាប់(Links) ឬ ឯកសារ(Attachment) ដែលមិនស្គាល់ប្រភពច្បាស់លាស់នៅក្នុងអ៊ីម៉ែល ជាអាទិ៍
- ធ្វើការថតចម្លងទុកឯកសារជាប្រចាំ(Regular Backup) និងបិទការតភ្ជាប់អ៊ីនធឺណិត(Offline)
- ធ្វើការFormat នូវរាល់Hard drive នៅលើកុំព្យូទ័រណាដែលអ្នកចង់ឱ្យទៅគេ

កថាខណ្ឌទី ២ ទូរស័ព្ទដៃឆ្លាត (Smart phone)

ទូរស័ព្ទ មានមុខងារទូលំទូលាយ ដូចជាសម្រាប់ឆ្លើយឆ្លង ប្រើប្រាស់អ៊ីនធឺណិត ផ្ញើសារជាសម្លេង និងផ្ញើសាររហ័សភ្លាមៗ តាមអ៊ីនធឺណិត ចាប់យក រក្សាទុក និងបញ្ជូនសម្លេង រូបថត និងវីដេអូ ប្រើបណ្តាញទំនាក់ទំនងសង្គម លេងហ្គេម ប្រើសេវាធនាគារ សូម្បីតែព័ត៌មានទាក់ទងនឹងវីរុសកូវីដ-១៩ ដែលកំពុងកើតរីករាលដាលនាពេលបច្ចុប្បន្នក៏ជាផ្នែកមួយដែលយើងទទួលបានដោយសារទូរស័ព្ទ ព្រមទាំងសកម្មភាពជាច្រើនផ្សេងទៀត ។ ក៏ប៉ុន្តែ កម្មវិធីនិងមុខងារជាច្រើនទាំងនេះ នាំមកនូវបញ្ហាសុវត្ថិភាពថ្មី ឬ បង្កើនកម្រិតហានិភ័យដែលមានស្រាប់ផងដែរ ។ ដើម្បីការពារទូរស័ព្ទអ្នកប្រឆាំងនឹងបទល្មើសបច្ចេកវិទ្យា យើងមានយុទ្ធសាស្ត្រឈ្នះឈ្នះចំនួន ៦(ប្រាំ) ដែលយុត្តិសាស្ត្រទាំងនោះរួមមាន **ចាក់សោរអេក្រង់**(២.១) **តម្លើងកម្មវិធីកម្ចាត់មេរោគ**(២.២) **ប្រុងប្រយ័ត្នចំពោះវាយហ្វាយ**(២.៣) **ថតចម្លងទិន្នន័យទុកមុនជានិច្ច**(២.៤) **ត្រូវធ្វើបច្ចុប្បន្នភាពប្រតិបត្តិការទូរស័ព្ទដៃ**(២.៥) និង **កុំដំឡើងកម្មវិធីដែលមានប្រភពមិនច្បាស់លាស់**(២.៦) ។

២.១ ចាក់សោរអេក្រង់

[52]សេចក្តីជូនដំណឹងទាក់នឹងសេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន, លេខ ៤២ បទ.សជណ, ២៥ ឧសភា ២០២១។

សោអេក្រង់ជារនាំងការពារដំបូងបំផុត ដោយការពារមិនឱ្យបុគ្គលដទៃអាចចូលមើលទិន្នន័យដូចជា រូបថត កម្មវិធី និងទិន្នន័យ ជាអាទិ៍ ដែលមាននៅលើទូរសព្ទ័របស់អ្នកដោយមិនមានការអនុញ្ញាត ។ ជាទូទៅ ការចាក់សោលើទូរស័ព្ទមានច្រើនប្រភេទ ។ ជាទូទៅការចាក់ចោសោលើទូរស័ព្ទមានច្រើនប្រភេទ ក្នុងនោះរួម មាន លេខកូដសម្ងាត់(Password) លេខ៤ខ្ទង់(PIN) គំនូសសញ្ញា(Pattern) ស្នាមខ្ចៅដៃ(Fingerprint) និងស្កែនមុខ(FaceID) ជាដើម ។

២.២ ដំឡើងកម្មវិធីកម្ចាត់មេរោគ

ទន្ទឹមនឹងការប្រើប្រាស់ទូរស័ព្ទនៅកម្ពុជា កើនឡើងជាលំដាប់ និងមានច្រើនម៉ាកផងនោះ កម្មវិធីទូរស័ព្ទ ច្រើនក៏ត្រូវបានបង្កើតឡើងដែរ ។[53] មិនមែនកម្មវិធីទាំងអស់សុទ្ធតែល្អនោះទេ មានកម្មវិធីមួយចំនួនត្រូវបាន បង្កើតឡើងដោយក្រុមហេកគ័រ និងបានបង្កប់ម៉ាលវែ(Malware) ឬ មេរោគនៅក្នុងនោះ ។ ល្អីកនេះ អ្នកគួរ ដំឡើងកម្មវិធីកម្ចាត់មេរោគ ឬ កម្មវិធីកម្ចាត់ម៉ាលវែ(Malware) លើឧបករណ៍របស់អ្នក ដើម្បីការពារទូរស័ព្ទ របស់អ្នកឱ្យមានសុវត្ថិភាពប្រឆាំងនឹងបទល្មើសព័ត៌មានវិទ្យា ។

២.៣ ប្រុងប្រយ័ត្នចំពោះWifi

Wifi គឺអាចជាច្រកមួយដែលចោរព័ត៌មានវិទ្យាអាចភ្ជាប់មកទូរស័ព្ទដៃរបស់អ្នកបាន ដើម្បីការពារ សុវត្ថិភាពអ្នកគួរជៀសវាងការភ្ជាប់បណ្តាញWifi នៅទីសាធារណៈ ឬ Wifiមិនមានសុវត្ថិភាព(មិនមានពាក្យ សម្ងាត់ដើម្បីភ្ជាប់ចូល) ។ ក្នុងករណីអ្នកត្រូវប្រើWifi នៅទីសាធារណៈជាចាំបាច់ អ្នកគួរពិនិត្យ និងភ្ជាប់ បណ្តាញដែលអ្នកគិតថាអាចមានសុវត្ថិភាព ហើយមិនត្រូវធ្វើប្រតិបត្តិការហិរញ្ញវត្ថុ ឬ ចូលប្រើប្រាស់ទិន្នន័យ សំខាន់ឡើយ ។

២.៤ ថតចម្លងទិន្នន័យទុកមុនជានិច្ច

មិនថាទូរស័ព្ទរបស់អ្នកត្រូវបានបាត់ ឬ ខូច ឬ អាចត្រូវចោរបច្ចេកវិទ្យាវាយប្រហារនោះទេ វាជាការចាំ បាច់បំផុតដែលអ្នកត្រូវមានការថតចម្លងទុកទិន្នន័យចេញពីទូរស័ព្ទរបស់អ្នក អ្នកអាចចម្លងទុកព័ត៌មានយកទៅ ផ្ទុកក្នុងកុំព្យូទ័រ ឬ ផ្ទុកនៅលើក្លោដ(cloud-based service) អាស្រ័យលើប្រភេទទូរស័ព្ទរបស់អ្នក ។ ទូរស័ព្ទខ្លះ អាចមានមុខងារដើម្បីបញ្ជាលុបទិន្នន័យ ឬ ព័ត៌មានពីចម្ងាយពីក្នុងទូរស័ព្ទដៃរបស់អ្នក ហេតុនេះការថតចម្លង ទុកព័ត៌មានជាយុទ្ធសាស្ត្រដ៏ល្អប្រសើរមួយដើម្បីជួយរក្សាព័ត៌មានរបស់អ្នក ។

២.៥ ធ្វើបច្ចុប្បន្នភាពប្រព័ន្ធប្រតិបត្តិការទូរស័ព្ទដៃ

ទោះជាទូរស័ព្ទអ្នកម៉ូដែលណាក៏ដោយ អ្នកត្រូវប្រាកដថាប្រព័ន្ធប្រតិបត្តិការ និងគ្រប់កម្មវិធីទាំងអស់នៅ ក្នុងទូរស័ព្ទអ្នកធ្វើបច្ចុប្បន្នភាពជាមួយនឹងជំនាន់ចុងក្រោយបង្អស់ ។ ការធ្វើបច្ចុប្បន្នភាពទូរស័ព្ទវាជួយជួសជុល

[53]សូមមើល ឧបសម្ព័ន្ធ នៃសារណានេះ

នូវចំនុចខ្សោយ ឬ កង្វះខាតរបស់កម្មវិធីជំនាន់មុន និងជួយពង្រឹងផ្នែកសុវត្ថិភាពនៃប្រព័ន្ធប្រតិបត្តិការ ឬ កម្មវិធីនោះ ។ អ្នកគួរតែកំណត់បើកមុខងារក្នុងការធ្វើបច្ចុប្បន្នភាពដោយស្វ័យប្រវត្តិនៅក្នុងទូរស័ព្ទអ្នក ។ ប្រសិនបើអ្នករកឃើញថា ទូរស័ព្ទរបស់អ្នកលែងទទួលបានការធ្វើបច្ចុប្បន្នភាព ដោយសារតែទូរស័ព្ទនោះចាស់ពេក នោះអ្នកគួរតែពិចារណាប្តូរទូរស័ព្ទថ្មី ។ យុទ្ធសាស្ត្របែបនេះ ក៏មានប្រសិទ្ធភាពផង ក្នុងករណីដែលអ្នកប្រើប្រាស់មិនបានធ្វើបច្ចុប្បន្នភាពទេនោះ ជាទូទៅទូរស័ព្ទដៃ អាចប្រឈមនឹងការវាយប្រហារបានដោយមិនពិបាក ។

២.៦ កុំតម្លើងកម្មវិធីដែលមានប្រភពមិនច្បាស់លាស់

ទូរស័ព្ទរបស់អ្នកអាចឆ្លងមេរោគ ប្រសិនបើអ្នកទាញយកកម្មវិធីទាំងនោះពីគេហទំព័រដែលមានប្រភពមិនច្បាស់លាស់ ។ មេរោគទាំងនោះអាចមានលទ្ធភាពក្នុងការលួចយកទិន្នន័យពីក្នុងទូរស័ព្ទអ្នកបាន ។ ដើម្បីកាត់បន្ថយពីភាពរងគ្រោះនេះ អ្នកត្រូវទាញកម្មវិធីតែពីPlay store សម្រាប់ទូរស័ព្ទប្រភេទ Android និង App store សម្រាប់ទូរស័ព្ទប្រភេទiOS ។ បន្ថែមពីលើនេះ អ្នកគួរដឹងថា កម្មវិធីណាដែលអ្នកត្រូវការជាចាំបាច់ សម្រាប់ប្រើប្រាស់នៅក្នុងទូរស័ព្ទរបស់អ្នក ។ អ្នកគួរលុបកម្មវិធីណាដែលអ្នកមិនចាំបាច់ប្រើប្រាស់ពីព្រោះវាអាចជួយធ្វើឱ្យប្រព័ន្ធទូរស័ព្ទរបស់អ្នកមានដំណើរការលឿនជាមុន និងកាត់បន្ថយក្នុងការបាត់បង់នូវឯកជនភាព ។ គួសបញ្ជាក់ថា ការដែលយើងតម្លើងកម្មវិធីណាមួយដែលមិនមានប្រភពច្បាស់លាស់ កម្មវិធីដែលអ្នកបានតម្លើងនោះនឹងស្រង់យកទិន្នន័យពីអ្នក ហើយទិន្នន័យទាំងនោះ អាចជាកម្មវត្ថុនៃការលក់ដោយចោរបច្ចេកវិទ្យា ។ ល្អីកនេះ អ្នកមិនត្រូវតម្លើងកម្មវិធីមួយណាដែលមិនមានប្រភពច្បាស់លាស់នោះទេ ។

ផ្នែកទី ២ យុទ្ធសាស្ត្រឈ្លះឈ្លះសម្រាប់អ្នកប្រើប្រាស់បណ្តាញសង្គម

បណ្តាញសង្គម គឺជាបច្ចេកវិទ្យាដែលសម្របសម្រួលដោយកុំព្យូទ័រជួយសម្រួលដល់ការបង្កើត និងចែករំលែកព័ត៌មាន គំនិត ចំណាប់អារម្មណ៍ពីការងារ និងទម្រង់នៃការបញ្ចេញមតិផ្សេងៗទៀត តាមរយៈសហគមន៍ន៍និងបណ្តាញនិម្មិត(វើធ្យូ) ។[54] គិតត្រឹមដើមឆ្នាំ២០២១ នេះ មានអ្នកប្រើប្រាស់បណ្តាញសង្គមរហូតទៅដល់ចំនួន ១២(ដប់ពីរលាន) នាក់ ពោលគឺមានការកើនឡើង២៤% (ម្ភៃបួន) ភាគរយបើគិតពីឆ្នាំ ២០២០ មក ។[55] បច្ចុប្បន្នបណ្តាញសង្គម បានដើរតួនាទីជាផ្នែកមួយនៃសកម្មភាពជីវិតរបស់អ្នកប្រើប្រាស់ដើម្បីជាប្រយោជន៍របស់ខ្លួន ។ ក៏ប៉ុន្តែអ្នកប្រើប្រាស់អាចមិនបានកត់សម្គាល់ថាបណ្តាញសង្គមអាចបង្កហានិភ័យដល់ខ្លួន ។ ហានិភ័យនេះយើងចង់សំដៅអំពីការវាយប្រហាររបស់ចោរបច្ចេកវិទ្យា ជាអាទិ៍ ។ មែនទែនទៅ បណ្តាញសង្គមមានមិនតិចទេនៅកម្ពុជាដែលប្រជាពលរដ្ឋកំពុងតែប្រើប្រាស់ ដែលក្នុងនោះរួម

[54]គណៈកម្មាធិការសហប្រតិបត្តិការដើម្បីកម្ពុជា, ក្រមប្រតិបត្តិបច្ចេកវិទ្យាព័ត៌មានវិទ្យា និងទំនាក់ទំនង សម្រាប់បណ្តាញសង្គម, (២០១៨), ទំព័រទី១៤។

[55]https://datareportal.com/reports/digital-2021-cambodia (ចូលទស្សនានៅថ្ងៃទី ១៦ ខែឧសភា ឆ្នាំ២០២១)។

មាន **Facebook Telegram Intragram Tictok Twitter Email Wechat Youtube Line Snapchat** ជាដើម ។[56] ក៏ប៉ុន្តែ ដោយសារបណ្តាញសង្គម មានភាពស្រដៀងគ្នាចំពោះយុទ្ធសាស្ត្រក្នុងការពារខ្លួនដើម្បីប្រឆាំងនឹងបទល្មើសព័ត៌មាន ។ ម្ល៉ោះហើយ នៅក្នុងផ្នែកទី២ យើងនឹងលើកយុទ្ធសាស្ត្រឈ្នះឈ្នះប្រឆាំងនឹងបទល្មើសព័ត៌មានសម្រាប់អ្នកប្រើប្រាស់បណ្តាញ**ហ្វេសប៊ុក**(កថខណ្ឌទី១) និង**តេលេក្រាម**(កថាខណ្ឌទី២) ។

កថាខណ្ឌទី ១ ហ្វេសប៊ុក(Facebook)

ហ្វេសប៊ុក(Facebook) ត្រូវបានបង្កើតឡើងនៅឆ្នាំ២០០៤ ដោយសហស្ថានិកចំនួនបួននាក់ គឺ លោក **Mark Zuckerberg**, **Eduardo Severin**, **Dustin Moskovitz** និង **Chris Hughes** ។[57] គួសបញ្ជាក់ថា មានអ្នកប្រើប្រាស់ហ្វេសប៊ុក(Facebook) សកម្មប្រចាំខែប្រហែល **២.៨៥0.000.000 (ពីរពាន់ប្រាំបីរយហាសិបលាន) នាក់** គិតត្រឹម**ត្រីមាសទី ១ (មួយ) ឆ្នាំ២០២១** ។[58] ក្នុងនោះដែល អ្នកប្រើប្រាស់ហ្វេសប៊ុក(Facebook) នៅកម្ពុជាគិតត្រឹមដើមនៃឆ្នាំ២០២១ នេះមានចំនួន **១១.៨៨៣.000 (ដប់មួយលានប្រាំបីសែនប្រាំបីម៉ឺនបីពាន់) នាក់** ។[59]

អ្នកប្រើប្រាស់ហ្វេសប៊ុកនៅកម្ពុជានាពេលបច្ចុប្បន្ន កំពុងតែចែករំលែកព័ត៌មានឯកជនរបស់ខ្លួនជាមួយមិត្តភក្តិ និងក្រុមគ្រួសារ ជាអាទិ៍។ ជាអកុសលព័ត៌មានផ្ទាល់ខ្លួនមួយចំនួនដែលត្រូវបានបង្ហោះនោះអាចត្រូវបានប្រើដោយចោរបច្ចេកវិទ្យាដើម្បីហែកគណនីធនាគាររបស់អ្នក លួចអត្តសញ្ញាណ លួចទិន្នន័យ លុបទិន្នន័យ ឬ ប្រព្រឹត្តបទល្មើសផ្សេងទៀតដែលច្បាប់បានហាមឃាត់ ជាអាទិ៍ ។ ដើម្បីការពារហ្វេសប៊ុករបស់អ្នក ប្រឆាំងនឹងបទល្មើសព័ត៌មានវិទ្យា យុទ្ធសាស្ត្រទាំងនោះរួមមាន **ត្រូវធ្វើការរក្សានូវព័ត៌មានផ្ទាល់ខ្លួនឱ្យមានលក្ខណៈឯកជន**(១.១) **ត្រូវជៀសវាងការក្បាទុកលេខកូដគណនីហ្វេសប៊ុករបស់អ្នកនៅលើឧបករណ៍សាធារណៈ**(១.២) **បើកលេខកូដសំងាត់ទី២**(១.៣) **ត្រូវប្រើពាក្យសំងាត់ដែលរឹងមាំ**(១.៤) **ត្រូវប្រុងប្រយ័ត្នរាល់ពេលភ្ជាប់ទៅកាន់Wifiទីសាធារណៈ**(១.៥) **ត្រូវប្រុងប្រយ័ត្នមុនពេលចុចលើតំណរភ្ជាប់ណាមួយ** (១.៦) ។

១.១ ត្រូវធ្វើការរក្សានូវព័ត៌មានផ្ទាល់ខ្លួនឱ្យមានលក្ខណៈឯកជន

យើងមិនត្រូវធ្វើការបង្ហោះនូវឈ្មោះក្រុមគ្រួសាររបស់អ្នកទាំងអស់ ដោយសារតែវាអាចត្រូវបានប្រើប្រាស់ដើម្បីទស្សទាយនូវសំនួរសំងាត់ ឬ ក៏ទាញជាពាក្យសម្ងាត់របស់អ្នក ។ ទៀតនោះផងដែល សូមកុំធ្វើបង្ហោះនូវឈ្មោះសាលាដែលអ្នកបានសិក្សា ទីកន្លែងកំណើតដែលអ្នកកើត ឬ ទីកន្លែងដែលអ្នកធ្វើការ ជាអាទិ៍ ។

[56] https://blog.hootsuite.com/best-social-media-apps-list/ (ចូលទស្សនានៅថ្ងៃទី ២៩ ខែឧសភា ឆ្នាំ២០២១)។

[57] https://www.britannica.com/topic/Facebook (ចូលទស្សនានៅថ្ងៃទី ២៩ ខែឧសភា ឆ្នាំ២០២១)។

[58] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (ចូលទស្សនានៅថ្ងៃទី ១៦ ខែឧសភា ឆ្នាំ២០២១)។

[59] https://napoleoncat.com/stats/facebook-users-in-cambodia/2021/01 (ចូលទស្សនានៅថ្ងៃទី ១៦ ខែឧសភា ឆ្នាំ២០២១)។

ព័ត៌មានទាំងនេះត្រូវបានប្រើប្រាស់ជាទូទៅ ដើម្បីធ្វើការឆ្លើយទៅនឹងសំនួរសម្ងាត់នៅពេលដែលអ្នកភ្លេច ។

១.២ ត្រូវជៀសវាងការរក្សាទុកលេខកូដគណនីហ្វេសប៊ុករបស់អ្នកនៅលើឧបករណ៍សាធារណៈ

លេខកូដគណនីហ្វេសប៊ុក គឺបេះដូងនៃគណនី ។ ល្អីកនេះ ប្រសិនបើអ្នកបានប្រើប្រាស់ឧករណ៍សាធារណៈរួចហើយ អ្នកត្រូវតែលុបចោល ឬ សម្អាតទិន្នន័យនៃការប្រើប្រាស់នោះចេញ ។ ម្យ៉ាងវិញទៀត ត្រូវជៀសវាង មិនត្រូវរក្សាលេខកូដគណនីហ្វេសប៊ុកនៅលើឧបករណ៍សាធារណៈនោះទេ ដោយហេតុថាសកម្មភាពបែបនេះ គឺបង្កភាពងាយស្រួលដល់ចោរបច្ចេកវិទ្យាក្នុងការធ្វើប្រតិបត្តិនៃបទល្មើស ។

១.៣. បើកលេខកូដសំងាត់ទី ២

នៅពេលដែលយើងបានបើកលេខសំងាត់ទីពីរនៅក្នុងគណនីហ្វេសប៊ុករបស់អ្នក មានន័យថានៅពេលដែលមាននរណាម្នាក់ព្យាយាមហែកយកគណនីរបស់យើង ពេលនោះក្រុមហ៊ុនហ្វេសប៊ុកនឹងផ្ញើលេខលេខកូដទី២ នេះតាមរយៈលេខទូរស័ព្ទ ឬ តាមរយៈEmail ដែលយើងបានកំណត់នៅក្នុងហ្វេសប៊ុកស្រាប់ ។ គួសបញ្ជាក់ថា បើចោរបច្ចេកវិទ្យាមានលេខសម្ងាត់នៃគណនីហ្វេសប៊ុកយើងហើយក៏ដោយ ក៏ចោរបច្ចេកវិទ្យានោះមិនអាចចូលគណនីហ្វេសប៊ុកយើងបានទេ មានតែយើងទេដែលមានលេខកូដនោះ ។ ដើម្បីដំឡើងលេខសំងាត់ទី២ ដំបូងត្រូវចូលកម្មវិធីហ្វេសប៊ុក រួចចុច Setting and Privacy ហើយចុចយកពាក្យSetting បន្ទាប់មកជ្រើសយកពាក្យSecurity and Login ហើយចុចត្រង់ពាក្យថាប្រើប្រាស់លេខសំងាត់ទី២(Use two-factor authentication) និងជ្រើសរើសវិធីក្នុងការផ្ទៀងផ្ទាត់2FA(Select a Security Method) តាមរយៈកម្មវិធី Google Authenticator ឬ លេខទូរស័ព្ទរបស់អ្នក ។ ប្រសិនបើអ្នកចង់ឱ្យមានដើម្បីងាយស្រួលអ្នកអាចជ្រើសរើសយកសារ (SMS) ហើយចុចលើពាក្យថាបន្ត រួចវាយបញ្ចូលលេខទូរស័ព្ទរបស់អ្នក ហើយចុចខមហ្សម ។ ក្រោយពីធ្វើបែបនេះលេខកូដនឹងបញ្ជូនទៅកាន់លេខទូរស័ព្ទរបស់អ្នកសូមវាយបញ្ចូលលេខកូដនោះក្នុងComfirmកូដ ហើយចុចពាក្យថាបន្ទាប់ ។ **ចំណាំ** បន្ទាប់ពីដំឡើងលេខសំងាត់ទី២ រាល់ការចូលប្រើប្រាស់គណនីហ្វេសប៊ុករបស់អ្នកពីកម្មវិធី ឬ កុំព្យូទ័រថ្មី តម្រូវឱ្យមានការវាយបញ្ចូលលេខសម្ងាត់ និងលេខកូដដែលផ្ញើទៅកាន់លេខទូរស័ព្ទទើបអាចប្រើប្រាស់គណនីហ្វេសប៊ុកបាន ។

១.៤. ត្រូវដាក់ពាក្យសម្ងាត់រឹងមាំ(Strong Password)

ពាក្យសម្ងាត់ដែលរឹងមាំ គឺជាពាក្យសម្ងាត់ដែលមានប្រវែងយ៉ាងតិចឱ្យបានពី៨(ប្រាំបី)ទៅ១២(ដប់ពីរ)តួរអក្សរ ប៉ុន្តែប្រសិនបើមានចំនួន២០(ម្ភៃ)តួរអក្សរ ឬ វែងជាងនេះកាន់តែល្អ ។ ជាងនេះពាក្យសម្ងាត់ ជាពាក្យសម្ងាត់ដែលមានភាពស្មុគស្មាញ ដោយលាយបញ្ចូលគ្នារវាងលេខ អក្សរ(តូច ធំ) និងនិមិត្តសញ្ញាផ្សេងៗ ។ ខ្ញុំសូមបញ្ជាក់ថា ពាក្យសម្ងាត់នោះ ជាឃ្លាដែលងាយចាំសម្រាប់អ្នក ។ ដើម្បីឱ្យកាន់តែច្បាស់យើងសូមលើក

ឧទាហរណ៍៖ 4JuUe*+9!OUY^ ឬ G#dod8%^lEcT64 ។

១.៥ ត្រូវប្រុងប្រយ័ត្នរាល់ពេលភ្ជាប់ទៅកាន់Wifiសាធារណៈ

ការប្រើប្រាស់Wifiនៅទីសាធារណៈ ជួយកាត់បន្ថយចំណាយកញ្ចប់អ៊ីនធឺណិតរបស់អ្នកប្រើប្រាស់ ប៉ុន្តែមានហានិភ័យមួយចំនួនដូចជា ការលួចស្តាប់យកទិន្នន័យចរាចរណ៍ ការជ្រៀតចូលម៉ាស៊ីនកុំព្យូទ័រ ការលួចយកលេខសម្ងាត់គណនី និងជ្រៀតចូលប្រព័ន្ធ ជាអាទិ៍ ។ វាយហ្វាយ នៅតាមទីសាធារណៈមានមនុស្សចម្រុះប្រើប្រាស់ ដូច្នេះមុននឹងអ្នកធ្វើការភ្ជាប់វាយហ្វាយ អ្នកត្រូវគិតពិចារណាអំពីថាតើ វាយហ្វាយនោះអ្នកស្គាល់ដែលឬទេ ធ្វើបែបនេះគឺដើម្បីសុវត្ថិភាព ពីព្រោះជាទូទៅចោរបច្ចេកវិទ្យាតែងតែវាយប្រហារនៅពេលអ្នកភ្លេចខ្លួនជាអាទិ៍ ។[60]

១.៦ ត្រូវប្រុងប្រយ័ត្នមុននឹងធ្វើការចុចលើតំណភ្ជាប់(Link) **ណាមួយ**

អ្នកត្រូវគិតពិចារណាឱ្យបានច្បាស់លាស់មុននឹងចុចទៅលើតំណភ្ជាប់ណាមួយ ពីព្រោះថាមិនមែនគ្រប់តំណភ្ជាប់ទាំងអស់មិនមានមេរោគទាំងអស់នោះទេ ។ ជាងនេះ អ្នកត្រូវដឹងអំពីប្រភពនៃតំណភ្ជាប់នេះថាអ្នកណាផ្ញើមក មិត្តភក្តិ គ្រួសារ លោកគ្រូអ្នកគ្រូ ជាដើម មុននឹងធ្វើការចុចទៅលើតំណភ្ជាប់នោះ ។ ការធ្វើបែបនេះមានអត្ថប្រយោជន៍ណាស់ ព្រោះថាបើយើងមិនចុចតំណភ្ជាប់នោះទេ នោះមេរោគរបស់ចោរបច្ចេកវិទ្យានឹងមិនអាចជ្រៀតចូលក្នុងគណនីហ្វេសប៊ុករបស់អ្នកដែរ ។

កថាខណ្ឌទី ២ តេលេក្រាម(Telegram)

តេលេក្រាម(Telegram) ជាប្រព័ន្ធកម្មវិធីផ្ញើសារដោយឥតគិតថ្លៃតាមរយៈប្រព័ន្ធអ៊ីនធឺណិត ដែលកំពុងមានការទន្ទឹមនឹងការពេញនិយមនេះ ក៏ជាឱកាសមួយដែលចោរបច្ចេកវិទ្យា ឬ ហែកគ័រ បានធ្វើការវាយប្រហារក្រោមរូបភាពផ្សេងៗដូចជា ការលួចចូលគណនីរបស់អ្នកប្រើប្រាស់ ការបោកបញ្ឆោតផ្សេងៗ ដោយផ្ញើតំណភ្ជាប់ ឬ ឯកសារដែលមានផ្ទុកមេរោគ ក្នុងគោលបំណងលួចយកព័ត៌មានសំខាន់ៗ ឬ ចម្លងមេរោគចូលក្នុងឧបករណ៍របស់អ្នកប្រើប្រាស់ដើម្បីធ្វើការគ្រប់គ្រងទាំងស្រុងតែម្តង ។ ចំណុចសំខាន់មួយបន្ទាប់ពីបង្កើតគណនីតេលេក្រាម គឺបញ្ហាសុវត្ថិភាព អ្នកប្រើប្រាស់គួរមានការយល់ដឹងអំពីយុទ្ធសាស្ត្រឈ្នះឈ្នះការពារតេលេក្រាមរបស់អ្នក ដើម្បីប្រឆាំងនឹងបទល្មើសព័ត៌មានវិទ្យា ។ ហេតុដូច្នេះហើយ យើងសូមលើកយកយុទ្ធសាស្ត្រឈ្នះឈ្នះចំនួន៦(ប្រាំមួយ) ដើម្បីការពារតេលេក្រាមរបស់អ្នកប្រឆាំងនឹងបទល្មើសព័ត៌មានវិទ្យាបាន ដែលយុទ្ធសាស្ត្រទាំងនោះរួមមាន **ត្រូវប្រើមុខងារផ្ទៀងផ្ទាត់ពីរជំហាន**(២.១) **ត្រូវពិនិត្យមើល Active Sessions** (២.២) **ប្រើមុខងារ Passcode Lock**(២.៣) **កុំអើពើនឹងសារក្លែងក្លាយ**(២.៤) **ត្រូវប្រើពាក្យសម្ងាត់រឹងមាំ**(២.៥) **ប្រុងប្រយ័ត្នពីការបោកបញ្ឆោត**(២.៦) ។

[60] [សុវត្ថិភាពនៃការប្រើប្រាស់ Wifi សាធារណៈ :– SecuDemy.com](#) (ចូលទស្សនានៅថ្ងៃទី ១០ ខែឧសភា ឆ្នាំ២០២១)។

២.១ ប្រើមុខងារផ្ទៀងផ្ទាត់ពីរជំហាន

ជាទូទៅការបង្កើតគណនីតេលេក្រាម គឺគ្រាន់តែបញ្ចូលលេខទូរស័ព្ទ និងលេខកូដដែលទទួលបានប៉ុណ្ណោះ ។ ប្រសិនបើចោរបច្ចេកវិទ្យា ឬ ហេកគ័រ អាចលួចបានលេខកូដនេះតាមវិធីសាស្ត្រណាមួយ គណនីរបស់អ្នកប្រើប្រាស់អាចនឹងត្រូវបានចោរបច្ចេកវិទ្យាលួចចូលបាន ។ ដើម្បីការពារគណនី អ្នកប្រើប្រាស់គួរប្រើមុខងារផ្ទៀងផ្ទាត់ពីរជំហាន ដោយមុខងារនេះតម្រូវឱ្យមានការផ្ទៀងផ្ទាត់បន្ថែមមួយទៀតពីលើលេខកូដដែលទទួលបាន ។ អ្នកប្រើប្រាស់ត្រូវប្រើមុខងារនេះ ដោយអនុវត្តតាមការណែនាំដូចខាងក្រោម៖[61]

- បើកកម្មវិធី តេលេក្រាម ហើយចូលទៅគណនីរបស់អ្នក
- ចូលទៅកាន់ "Settings"
- ចុចលើ "Privacy and Security"
- បន្ទាប់មកចុចលើ "Two-Step Verification" បន្ទាប់មកចុចលើ "Set Password"
- ត្រង់ចំណុច "Enter a password" បញ្ចូលពាក្យសម្ងាត់ បន្ទាប់មកចុច "Continue" រួចហើយ ត្រង់ចំណុច "Re-enter your password" សូមបញ្ចូលពាក្យសម្ងាត់ដដែលម្តងទៀត រួចហើយចុចលើពាក្យ "Continue"
- បន្ទាប់មកត្រង់ចំណុច "Password Hint" អ្នកអាចបញ្ចូល ឬ មិនបញ្ចូលព័ត៌មាន ប្រសិនបើអ្នកបញ្ចូលសូមចុចលើ "Continue" ប្រសិនបើមិនបញ្ចូលសូមចុចលើ "Skip"។ ត្រង់ចំណុច "Password Hint" នេះគឺជាគន្លឹះសម្រាប់អ្នកប្រើប្រាស់អាចចងចាំទៅដល់ពាក្យសម្ងាត់ដែលបានដាក់ (ដែលព័ត៌មាននឹងបង្ហាញជាសាធារណៈ)
- បន្ទាប់មកត្រង់ចំណុច "Recovery Email" អ្នកអាចបញ្ចូល ឬ មិនបញ្ចូលព័ត៌មាន អាសយដ្ឋានអ៊ីម៉ែល ប្រសិនបើអ្នកបញ្ចូល សូមចុចលើ "Continue" ប្រសិនបើមិនបញ្ចូលសូមចុចលើ "Skip" ។ ត្រង់ចំណុចនេះអ្នកគួរភ្ជាប់អាសយដ្ឋានអ៊ីម៉ែល ដើម្បីអាចធ្វើការទាញយកពាក្យសម្ងាត់ថ្មីនៅពេលដែលភ្លេចពាក្យសម្ងាត់ដែលបានដាក់
- បន្ទាប់មកអ្នកត្រូវចូលទៅកាន់ប្រអប់សារអ៊ីម៉ែល ដែលបានដាក់ក្នុងចំណុចខាងលើ ដើម្បីឆែកមើលលេខកូដ៦(ប្រាំមួយ)ខ្ទង់ ដែលទទួលបានពីតេលេក្រាម និងបញ្ចូលលេខកូដនោះត្រង់ចំណុច "Verification code" បន្ទាប់ពីបញ្ចូលត្រឹមត្រូវមានន័យថាអ្នកបានបើកប្រើមុខងារនេះបានជោគជ័យ។

២.២ **ពិនិត្យមើល** (Active Sessions)

ពិនិត្យមើល (Active Sessions) ជាមុខងារមួយដែលអាចឱ្យអ្នកប្រើប្រាស់មើលរាល់ Sessions ទាំង

[61] https://www.camcert.gov.kh/telegram-security/ (ចូលទស្សនានៅថ្ងៃទី ២០ ខែមិថុនា ឆ្នាំ២០២១)។

អស់ដែលកំពុងប្រើប្រាស់គណនីតេលេក្រាមរបស់ខ្លួន អ្នកប្រើប្រាស់គួរពិនិត្យមើលថាតើមាន Active Sessions ណាមួយដែលគួរឱ្យសង្ស័យដែរឬទេ ដើម្បីពិនិត្យមើល សូមអនុវត្តតាមការណែនាំដូចខាងក្រោម៖[62]

- បើកកម្មវិធីតេលេក្រាមហើយចូលទៅគណនីរបស់អ្នក
- ចូលទៅកាន់ "Settings" បន្ទាប់មកចុចលើ "Devices"
- ពិនិត្យលើ Sessions ឬឧបករណ៍ទាំងអស់ដែលកំពុងប្រើគណនីរបស់អ្នក
- បើឃើញមាន Sessions ឬ ឧបករណ៍ ដែលសង្ស័យមិនមែនជារបស់អ្នក សូមចុចលើ Sessions ឬ ឧបករណ៍ ហើយចុចលើ "TERMINATE"
- បន្ទាប់មកអ្នកត្រូវផ្លាស់ប្តូរលេខសម្ងាត់ផ្ទៀងផ្ទាត់ពីរជំហានហើយ បន្តធ្វើការតាមដានមើល Session ឬ ឧបករណ៍ តាមការណែនាំខាងលើជារឿយៗដើម្បីពិនិត្យលើការប្រើប្រាស់ដែលមិនមែនជារបស់អ្នក ។

ប្រសិនបើអ្នកចុចលើ "TERMINATE ALL" នោះរាល់ឧបករណ៍ដែលបានភ្ជាប់ជាមួយគណនីរបស់ អ្នកនឹងត្រូវបានផ្តាច់ចេញពីគណនីទាំងអស់ លើកលែងតែឧបករណ៍ដែលអ្នកកំពុងប្រើប្រាស់ ។ ដូច នេះអ្នកគួរចុចបិទ(TERMINATE) តែឧបករណ៍ដែលមិនមែនជារបស់អ្នកប៉ុណ្ណោះ ។

២.៣ ប្រើមុខងារ Passcode Lock

តេលេក្រាម មានមុខងារដែលអនុញ្ញាតឱ្យអ្នកប្រើប្រាស់ចាក់សោកម្មវិធីដោយប្រើលេខកូដសម្ងាត់ ដើម្បី ការពារនៅពេលដែលនរណាចូលប្រើប្រាស់តេលេក្រាមនៅលើឧបករណ៍របស់ខ្លួន ដោយមុខងារនេះគឺតម្រូវឱ្យ មានការបញ្ចូលលេខកូដសម្ងាត់ ដើម្បីអាចប្រើប្រាស់តេលេក្រាមបាន ។ ដើម្បីបង្កើតលេខកូដសម្ងាត់ សូម អនុវត្តតាមការណែនាំដូចខាងក្រោម៖[63]

- ចូលទៅកាន់ "Settings" បន្ទាប់មកចុចលើ" "Privacy and Security"
- ត្រង់ចំណុច "Security" ចុចលើពាក្យ "Turn on local passcode" ឬ "Passcode Lock" ឬ "Passcode & Touch ID"
- បន្ទាប់មកវាយបញ្ចូលលេខកូដសម្ងាត់ និងបញ្ចូលលេខកូដម្តងទៀតដើម្បីផ្ទៀតផ្ទាត់
- អ្នកប្រើប្រាស់ត្រូវតែចងចាំលេខកូដសម្ងាត់ដែលបានដាក់ ដើម្បីបញ្ចូលលេខកូដនេះរាល់ពេលចូលប្រើ ប្រាស់តេលេក្រាម ។

សូមកត់សម្គាល់ផងដែរ នៅលើទូរស័ព្ទអ្នកប្រសិនបើមានមុខងារស្កែនក្រយៅដៃ អ្នកអាចប្រើប្រាស់

[62] សុវត្ថិភាពក្នុងការប្រើប្រាស់តេលេក្រាម (Telegram) – CamCERT – National CERT of Cambodia (ចូលទស្សនានៅថ្ងៃទី ២០ ខែមេសា ឆ្នាំ២០២១)។

[63] https://www.camcert.gov.kh/telegram-security/ (ចូលទស្សនានៅថ្ងៃទី ២០ ខែមិថុនា ឆ្នាំ២០២១)។

ការស្កែន "ស្នាមក្រយៅដៃ" ជំនួសឱ្យការវាយបញ្ចូលលេខកូដ ដើម្បីចូលប្រើប្រាស់តេលេក្រាម វាក៏ជួយអ្នកឱ្យចូលបានលឿន និងមានសុវត្ថិភាព ។

២.៤ កុំអើពើនឹងសារក្លែងក្លាយ

ត្រង់ចំណុចនេះ យើងគប្បីស្វែងយល់ថា តើអ្នកធ្លាប់ទទួលបានសារដែលសារសរសេរជាភាសាអង់គ្លេសថា "Your account has been temporarily closed. To verify your identity, click the link below" ហើយជាភាសាខ្មែរប្រែថា "គណនីរបស់អ្នកត្រូវបានបិទជាបណ្តោះអាសន្នដើម្បីបញ្ជាក់អត្តសញ្ញាណរបស់អ្នកសូមចុចតំណរភ្ជាប់ខាងក្រោម" ។[64] សូមចងចាំថា តេលេក្រាមមិនដែលស្នើសុំឱ្យអ្នកបញ្ជាក់ពីអត្តសញ្ញាណរបស់អ្នកទេ ប្រសិនបើអ្នកទទួលបានសារបែបនេះ ច្បាស់ណាស់ថាជាសារក្លែងក្លាយ ហើយអ្នកមិនត្រូវចុចលើតំណរភ្ជាប់ដែលមាននៅក្នុងសារនោះទេ ពោលអ្នកត្រូវតែប្លុកចោលតែម្តង ។

២.៥ ប្រើពាក្យសម្ងាត់រឹងមាំ

នៅក្នុងពិភពលោកសព្វថ្ងៃនេះយើងឃើញមានគណនីតេឡេក្រាម ជាច្រើនត្រូវបានវាយប្រហារដោយចោរបច្ចេកវិទ្យា ឬ ហេកគ័រ មូលហេតុសំខាន់មួយគឺការធ្វេសប្រហែស និងការប្រើប្រាស់ពាក្យសម្ងាត់ទន់ខ្សោយ ដូច្នេះអ្នកគួរបង្កើតនិងប្រើប្រាស់ពាក្យសម្ងាត់រឹងមាំ ខាងក្រោមនេះគឺជាគន្លឹះ៨(ប្រាំបី)ចំណុច ក្នុងការបង្កើតពាក្យសម្ងាត់រឹងមាំ និងមិនងាយទាយដឹង៖[65]

- បង្កើតលេខកូដសម្ងាត់របស់អ្នកអោយបានវែងយ៉ាងហោចណាស់១២(ដប់ពីរ)ខ្ទង់
- ធ្វើឱ្យលេខសម្ងាត់របស់អ្នកពិបាកទាយដឹង
- បញ្ចូលតួលេខរួម និមិត្តសញ្ញា អក្សរធំ និងអក្សរតូច
- ជៀសវាងការប្រើប្រាស់ព័ត៌មានផ្ទាល់ខ្លួន
- កុំប្រើឡើងវិញនូវពាក្យសម្ងាត់ដែលធ្លាប់ប្រើ
- រក្សាទុកពាក្យសម្ងាត់ឱ្យមានសុវត្ថិភាព
- ផ្លាស់ប្តូរពាក្យសម្ងាត់ឱ្យបានទៀងទាត់

២.៦ ប្រុងប្រយ័ត្នពីការចោកបញ្ឆោត

ដូចដែលបានរៀបរាប់រួចមកហើយថា ចោរបច្ចេកវិទ្យា ឬ ហែកគ័រ ព្យាយាមបោកបញ្ឆោតអ្នកប្រើប្រាស់តាមរយៈវិធីសាស្ត្រផ្សេងៗ ក្នុងនេះក៏មានសារបោកបញ្ឆោតផងដែរ ប្រសិនបើអ្នកទទួលបានសារពាក់ព័ន្ធការ

[64] សុវត្ថិភាពក្នុងការប្រើប្រាស់តេឡេក្រាម (Telegram) – CamCERT – National CERT of Cambodia (ចូលទស្សនានៅថ្ងៃទី ២០ ខែមេសា ឆ្នាំ២០២១)។

[65] https://www.camcert.gov.kh/8tips-secure-password/ (ចូលទស្សនានៅថ្ងៃទី ២០ ខែមេសា ឆ្នាំ២០២១)។

ជូនដំណឹងស្តីពីគណនី សូមធ្វើការពិនិត្យនិងផ្ទៀងផ្ទាត់សារដែលផ្ញើមកនោះ ថាពិតជាផ្ញើមកពីតេលេក្រាមដែរ ឬទេ។[66] ដើម្បីពិនិត្យមើលសារជូនដំណឹងដែលផ្ញើមកពីតេលេក្រាម អ្នកអាចពិនិត្យសញ្ញាគ្រីស(☑) ពណ៌ខៀវ ដែលមាននៅជាប់ឈ្មោះTelegram មានន័យថាប្រសិនបើមិនឃើញមានសញ្ញាគ្រីសទេ ប្រាកដជាគណនីក្លែងក្លាយ អ្នកអាចប្លុក និងរាយការណ៍វា ព្រោះតេឡេក្រាមមានសុវត្ថិភាពខ្ពស់ហើយចោរបច្ចេកវិទ្យា ឬ ហែកគ័រ ក៏បានប្រើវិធីនេះដើម្បីទទួលបានលេខសម្ងាត់គណនីរបស់អ្នកផងដែរ ។ សូមមានការប្រុងប្រយ័ត្នចំពោះការទទួលបានសារខ្លីនៅក្នុងTelegram ពីអ្នកមិនស្គាល់ហើយតាំងខ្លួនថាជាអ្នកនេះ ឬអ្នកនោះ ហើយឱ្យអ្នកចុចបើកមើលឯកសារណាមួយដែលភ្ជាប់មក ឬ ឱ្យអ្នកចុចទៅលើតំណភ្ជាប់ (link) ណាមួយឱ្យសោះ ។[67] ម្លោះហើយអ្នកត្រូវប្រុងកត់ចំណាំ និងធ្វើការកត់សម្គាល់ត្រង់ចំណុចនេះ ។

[66] សុវត្ថិភាពក្នុងការប្រើប្រាស់តេឡេក្រាម (Telegram) – CamCERT – National CERT of Cambodia (ចូលទស្សនានៅថ្ងៃទី ១៥ ខែមិថុនា ឆ្នាំ២០២១០)។

[67] https://www.camcert.gov.kh/be-aware-of-spear-phishing/ (ចូលទស្សនានៅថ្ងៃទី ២០ ខែមេសា ឆ្នាំ២០២១)

សេចក្តីសន្និដ្ឋាន

ឆ្លងតាមការបកស្រាយប្រធាន "បទល្មើសព័ត៌មានវិទ្យានៅកម្ពុជា" រួចមកយើងឃើញថា បទល្មើសព័ត៌មានវិទ្យា គឺជាបទល្មើសដែលប្រព្រឹត្តនៅក្នុងបណ្តាញបច្ចេកវិទ្យាគមនាគមន៍ និងព័ត៌មាននៃកម្ពុជា ដូចជា ការចូលលួច ក្លែងបន្លំ ឬកែឯកសារ ការបញ្ចូលមេរោគ ការផ្ញើសារគំរាមកំហែង ឬ ចាប់ជំរិត ឬ ការធ្វើឱ្យប៉ះពាល់ដល់សន្តិសុខសេដ្ឋកិច្ច និងសង្គមកិច្ច ។ បទល្មើសនេះពិតជាបង្កឱ្យមានព្យសនកម្មដល់សន្តិសុខ ចលាចល និងបង្កឱ្យមានភាពអសណ្តាប់ធ្នាប់សាធារណៈ ជាពិសេសអ្នកប្រើប្រាស់បច្ចេកវិទ្យា ឬ អ្នកប្រើប្រាស់បណ្តាញសង្គម ជាអាទិ៍ ។ ទៀតសោធនោះ បទល្មើសនេះកើតឡើងនៅក្នុងអ៊ីនធឺណិត ភ័ស្តុតាងក៏នៅក្នុងអ៊ីនធឺណិត មានន័យថាចារីមិនចាំបាច់ចេញទៅប្រព្រឹត្តបទល្មើសនៅទីតាំងណាមួយដោយផ្ទាល់នោះទេ ។

ដ្បិតបែបនេះក្តី កម្ពុជាយើងបានបង្កើតនូវស្ថាប័នជំនាញ ដើម្បីបង្ការ បង្ក្រាប ស្រាវជ្រាវ និងឆ្លើយតបចំពោះបញ្ហាដែលកើតមានទាក់ទងនឹងបទល្មើសព័ត៌មានវិទ្យា ពោលគឺនាយកដ្ឋានប្រឆាំងនឹងបទល្មើសបច្ចេកវិទ្យាដែលស្ថិតនៅក្រោមអគ្គស្នងការនគរបាលជាតិ នៃក្រសួងមហាផ្ទៃ និងការិយាល័យឆ្លើយតបបន្ទាន់នៃបញ្ហាកុំព្យូទ័រ ដែលស្ថិតនៅក្រោមនាយកដ្ឋានបច្ចេកវិទ្យាគនាគមន៍ និងព័ត៌មាន នៃអគ្គនាយកបច្ចេកវិទ្យា និងព័ត៌មាន នៃក្រសួងប្រៃសណីយ៍ និងទូរគមនាគមន៍ ។ បន្ថែមពីនេះ ទោះបីកម្ពុជាមិនទាន់មានច្បាប់ពិសេសក្តី ក៏កម្ពុជាមានក្របខណ្ឌច្បាប់ដែលមានចែងអំពីការផ្តន្ទាទោសសម្រាប់បុគ្គលដែលប្រព្រឹត្តបទល្មើសព័ត៌មានវិទ្យា ពោលគឺក្រមព្រហ្មទណ្ឌ ឆ្នាំ២០០៩ ចាប់ពីមាត្រា ៤២៧ ដល់ មាត្រា ៤៣២ ដែលបានបញ្ញត្តអំពី បទចូលទៅដល់ ឬ ស្ថិតនៅនឹងប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យ បទបង្កើតជាឧបសគ្គដល់ដំណើរការនៃប្រព័ន្ធប្រព្រឹត្តិកម្មស្វ័យប្រវត្តនៃទិន្នន័យ បទបញ្ចូល លុបបំបាត់ ឬ កែប្រែដោយទុច្ចរិតនូវទិន្នន័យ បទចូលរួមក្នុងក្រុមប្រមូលផ្តុំ ឬ ក្នុងសន្និដ្ឋិភាពដើម្បីរៀបចំប្រព្រឹត្តបទល្មើស ការប៉ុនប៉ង និងទោសបន្ថែម ។

លើលពីនេះ កម្ពុជាក៏កំពុងតែព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យា ដែលមាន ៦ ជំពូក និង ៤០ មាត្រា ។ សេចក្តីព្រាងច្បាប់នេះបានបញ្ញត្តិអំពីគោលបំណងនិងគោលដៅ បទល្មើស និងជំនួយផ្នែកច្បាប់ទៅវិញទៅមក និងកិច្ចសហប្រតិបត្តិការអន្តរជាតិនិងបត្យាប័ន ជាអាទិ៍ ។ សេចក្តីព្រាងច្បាប់នេះ បានធ្វើការប្រជុំអន្តរក្រសួងផង ប្រជុំជាមួយស្ថាប័ននៃរដ្ឋបរទេសផង ហើយកម្ពុជាថែមទាំងបានបញ្ជូនមន្ត្រីកម្ពុជាទៅកាន់រដ្ឋបរទេសដើម្បីទទួលបានចំណេះបន្ថែមទាក់ទងទៅនឹងក្របខណ្ឌច្បាប់ ការអនុវត្ត ទៅទស្សនាឧបករណ៍ទំនើបសម្រាប់ប្រើប្រាស់ស៊ើបអង្កេតកំណត់អត្តសញ្ញាណនៃជនល្មើស ពោលគឺដើម្បីយកចំណេះទាំងនោះមកឆ្លើយតបនឹងស្ថានភាពការវិវត្តនៃតថភាពសង្គមកម្ពុជាឱ្យដើរទាន់សភាពការណ៍ ។

ជាងនេះទៀត យើងក៏មានយុទ្ធសាស្ត្រឈ្នះឈ្នះដើម្បីប្រឆាំងនឹងបទល្មើសព័ត៌មានវិទ្យា ពោលគឺជាយុទ្ធសាស្ត្រឈ្នះឈ្នះសម្រាប់អ្នកប្រើប្រាស់កុំព្យូទ័រនិងទូរស័ព្ទ និងយុទ្ធសាស្ត្រឈ្នះឈ្នះសម្រាប់អ្នកប្រើ

ប្រាស់បណ្តាញសង្គម ។ យុទ្ធសាស្ត្រឈ្នះឈ្នះនេះ គឺទាមទារឱ្យអ្នកប្រើប្រាស់កុំព្យូទ័រនិងទូរស័ព្ទ និងអ្នកប្រើប្រាស់ បណ្តាញសង្គមត្រូវតែអនុវត្ត ទើបអាចប្រឆាំងនឹងបទល្មើសបច្ចេកវិទ្យាបាន ។

ជារួមមក បទល្មើសព័ត៌មានវិទ្យានៅកម្ពុជា គឺមានចែងតែនៅក្នុងក្រមព្រហ្មទណ្ឌកម្ពុជាតែប៉ុណ្ណោះ ហើយបទល្មើសនេះជាប្រភេទបទមជ្ឈិម ។ ដើម្បីអាចប្រឆាំងនឹងបទល្មើសព័ត៌មានវិទ្យា កម្ពុជាទាមទារឱ្យមានក្របខណ្ឌច្បាប់រឹងមាំ ស្តាប់ធ្នាញ ធនធានមនុស្ស ហិរញ្ញវត្ថុ ឧបករណ៍ទំនើប ជាអាទិ៍ ។

អនុសាសន៍

បច្ចេកវិទ្យា និងនវានុវត្តន៍ថ្មីៗបន្តរីកចម្រើននិងក្លាយជាឆ្អឹងខ្នងរបស់សេដ្ឋកិច្ចពិភពលោក ប៉ុន្តែវាក៏បានបង្កើតនិន្នាការថ្មី និងផ្តល់ឱកាសកាន់តែច្រើនសម្រាប់ចោរបច្ចេកវិទ្យាដើម្បីប្រព្រឹត្តបទល្មើសព័ត៌មានវិទ្យាតាមរយៈប្រព័ន្ធកុំព្យូទ័រ និងបណ្តាញអេឡិចត្រូនិក ជាអាទិ៍។ សន្តិសុខតាមអ៊ីនធឺណិតគឺជាបញ្ហាសកល ហើយកិច្ចប្រឹងប្រែងជាតិរបស់រដ្ឋនីមួយៗតែម្នាក់ឯងមិនអាចដោះស្រាយបញ្ហានេះបានជាដុំកំភួននោះទេ ។

ចំណែកឯសកលភាវូបនីយកម្ម និងការធ្វើសមាហរណកម្មតំបន់ កម្ពុជាត្រូវការច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន ដើម្បីធានាបាននូវសន្តិសុខតាមអ៊ីនធឺណិតនិងកិច្ចសហប្រតិបត្តិការអន្តរជាតិ ។ លើសពីនេះ ក៏បានបង្ហាញយ៉ាងច្បាស់ថាប្រទេសកម្ពុជាគួរតែត្រូវបានរៀបចំយ៉ាងល្អសម្រាប់ឱកាសខាងមុខសម្រាប់កំណើនសេដ្ឋកិច្ច និងការអភិវឌ្ឍ ។ ប្រទេសកម្ពុជាសម្រេចបាននូវកិច្ចខិតខំប្រឹងប្រែងសំខាន់ៗមួយចំនួនស្តីពីវិស័យព័ត៌មាន និងគោលនយោបាយ ពោលកម្ពុជាបានបង្កើតសេវាកម្មរដ្ឋាភិបាលអេឡិចត្រូនិក ពាណិជ្ជកម្មអេឡិចត្រូនិចនិងផ្តោតលើការលើកកម្ពស់ការយល់ដឹង និងការកសាងសមត្ថភាពដល់ប្រជាពលរដ្ឋ ជាអាទិ៍ ។

ពិតណាស់ សមិទ្ធផលកើតមានឡើងជាមួយនឹងបញ្ហាប្រឈមមួយចំនួន ។ កម្ពុជា នៅមានការខ្វះខាតច្បាប់ និងក្របខ័ណ្ឌយុទ្ធសាស្ត្រគោលនយោបាយ ដែលទាក់ទងទៅនឹងបទល្មើសព័ត៌មានវិទ្យា ដែលរារាំងប្រសិទ្ធភាពនៃការត្រួតពិនិត្យលើវិស័យព័ត៌មានវិទ្យានេះ ។

បើប្រៀបធៀបជាមួយប្រទេសដទៃទៀតនៅក្នុងតំបន់ ប្រទេសកម្ពុជានិងឡាវគឺជាប្រទេសយឺតបំផុតក្នុងការបង្កើតក្របខ័ណ្ឌច្បាប់ទាក់ទងនឹងវិស័យព័ត៌មានវិទ្យា ។ ទៀតសោតនោះ កម្ពុជាត្រូវការពង្រឹងនិងសម្របសម្រួលយន្តការក្នុងស្ថាប័នឱ្យមានប្រសិទ្ធភាពឆ្លើយតប ជាពិសេសធនធានមនុស្ស និងកម្រិតនៃចំណេះដឹងផ្នែកព័ត៌មានវិទ្យាដើម្បីទប់ទល់នឹងការរីកចម្រើនយ៉ាងឆាប់រហ័សនៃបច្ចេកវិទ្យាទំនើបៗ ។

ជាចុងក្រោយ ខ្ញុំបាទសូមជូនពាក្យមួយឃ្លាថា ប្រសិនបើមានតែការចូលរួមពីសំណាក់រដ្ឋាភិបាល ក៏ដូចជាស្ថាប័នដែលពាក់ព័ន្ធនោះក៏ដោយ ក៏មិនអាចកាត់បន្ថយនូវព្យសនកម្មដែលអាចកើតឡើងដោយសារតែបទល្មើសព័ត៌មានវិទ្យាឡើយ ពិតណាស់គឺទាមទារឱ្យប្រជាពលរដ្ឋទាំងអស់ ឈ្វេងយល់ដោយខ្លួនឯងបន្ថែមទើបជាការប្រសើរ ហើយត្រូវចាំថា គ្រប់បច្ចេកវិទ្យា ឬ បណ្តាញសង្គមទាំងអស់ មិនសុទ្ធតែសុវត្ថិភាពនោះទេ សុវត្ថិភាពកើតចេញពីខ្លួនអ្នក ។

ឯកសារយោង

ច្បាប់ និងបទដ្ឋានគតិយុត្ត

- រដ្ឋធម្មនុញ្ញ នៃព្រះរាជាណាចក្រកម្ពុជា ឆ្នាំ១៩៩៣ ។
- ក្រមព្រហ្មទណ្ឌ នៃព្រះរាជាណាចក្រកម្ពុជា, លេខ នស/រកម/១២០៧/០៣០, ០៨ ធ្នូ ២០០៧ ។
- ច្បាប់ស្តីពីទូរគមនាគមន៍, លេខ នស/រកម/១២១៩/០១៧, ១៧ ធ្នូ ២០១៥ ។
- ច្បាប់ស្តីពីពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក, លេខ នស/រកម/១១១៩/០១៧, ០២ វិច្ឆិកា ២០១៩ ។
- អនុក្រឹត្យ ស្តីពីការបង្កើតច្រកទ្វារអ៊ីនធឺណិតរាជរដ្ឋាភិបាល, លេខ ២៣ អនក្រ.បក, ១៦ កុម្ភៈ ២០២១ ។
- អនុក្រឹត្យ ស្តីពីការរៀបចំ និងការប្រព្រឹត្តទៅនៃក្រសួងមហាផ្ទៃ, លេខ ១០៩, ១៩ សីហា ២០១៥ ។
- សេចក្តីជូនដំណឹង, ក្រសួងប្រៃសណីយ៍ និងទូរគមនាគមន៍, លេខ ៤២ បទ.សជណ, ៣ កក្កដា ២០២១ ។
- ប្រកាសស្តីពី ការរៀបចំ និងការប្រព្រឹត្តទៅរបស់នាយកដ្ឋាន និងអង្គភាពក្រោមឱវាទអគ្គនាយកដ្ឋានបច្ចេកវិទ្យាគមនាគមន៍ និងព័ត៌មាន, លេខៈ ១២៥ បទ. ប្រក, ០២ មិថុនា ២០១៤ ។

សៀវភៅ

- ក្រុមប្រឹក្សាជាតិកម្ពុជាដើម្បីកុមារ, ផែនការសកម្មភាពដើម្បីបង្ការ ទប់ស្កាត់ និងឆ្លើយតបការកេងប្រវ័ញ្ចផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញ, ២០២១-២០២៥ ។
- ងួន សុម៉ាលី និងស្រ៊ុន សុភ័ក្ត្រ ,Cambodia V Hacker: តុល្យភាពរវាយសន្តិសុខ និងសេរីភាពនៅក្នុងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យា ។

គោលនយោបាយ និងក្របខណ្ឌគោលនយោបាយ

- គោលនយោបាយអភិវឌ្ឍន៍វិស័យទូរគមនាគមន៍ បច្ចេកវិទ្យាគមនាគមន៍ និងព័ត៌មាន ឆ្នាំ២០២០ ។
- ក្របខណ្ឌគោលនយោបាយសេដ្ឋកិច្ច និងសង្គមឌីជីថលកម្ពុជា, ២០២១ ដល់ ឆ្នាំ២០៣៥ ។

គេហទំព័រ

- ក្រសួងមហាផ្ទៃ https://www.interior.gov.kh/news/detail/2002
- ក្រសួងព័ត៌មាន https://www.information.gov.kh/articles/14898
- TechTarget https://searchsecurity.techtarget.com/definition/cybercrime
- នាយកដ្ឋានព័ត៌មានវិទ្យា នៃក្រសួងមហាផ្ទៃ IT.Department.MOI
- ការិយាល័យឆ្លើយតបបញ្ជាបន្ទាន់ នៃកុំព្យូទ័រ https://www.camcert.gov.kh
- សេកយ្យូឌីមីSecuDemy.com
- ណាប៉ូលេអុងខេត https://napoleoncat.com
- ខេបពីថលខេមប៉ូឌា https://capitalcambodia.com/how-cybercrime-affects-region/
- ប្រ៊ីដធេននីខា https://www.britannica.com/topic/Facebook
- ស្តេកតេសតា https://www.statista.com
- ទស្សនាវដ្តីបទល្មើសព័ត៌មានវិទ្យា https://cybersecurityventures.com cybercrime
- ដេលតារីផតថល https://datareportal.com/reports/digital-2021-cambodia

បញ្ជីឧបសម្ព័ន្ធ

ឧបសម្ព័ន្ធទី ១ ៖ ស្ថិតិទូរស័ព្ទដែលប្រើប្រាស់អ៊ីនធឺណិត

ឧបសម្ព័ន្ធទី ២ ៖ ស្ថិតិការប្រើប្រាស់ទូរស័ព្ទ

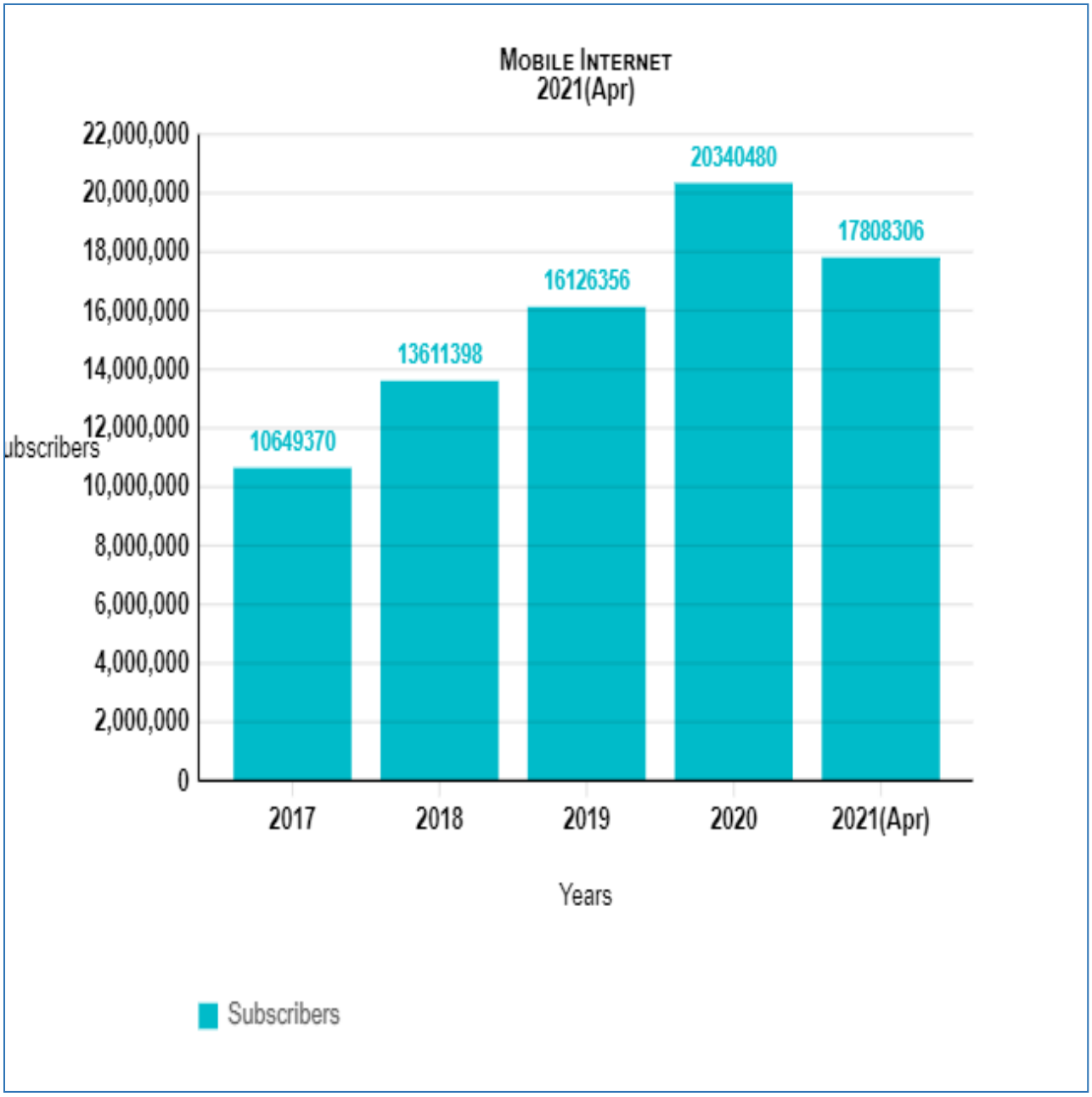
ឧបសម្ព័ន្ធទី ៣ ៖ សេចក្តីរាយការណ៍

ឧបសម្ព័ន្ធទី ៤ ៖ រចនាសម្ព័ន្ធក្រសួងមហាផ្ទៃ (នាយកដ្ឋានប្រឆាំងនឹងបទល្មើសបច្ចេកវិទ្យា)

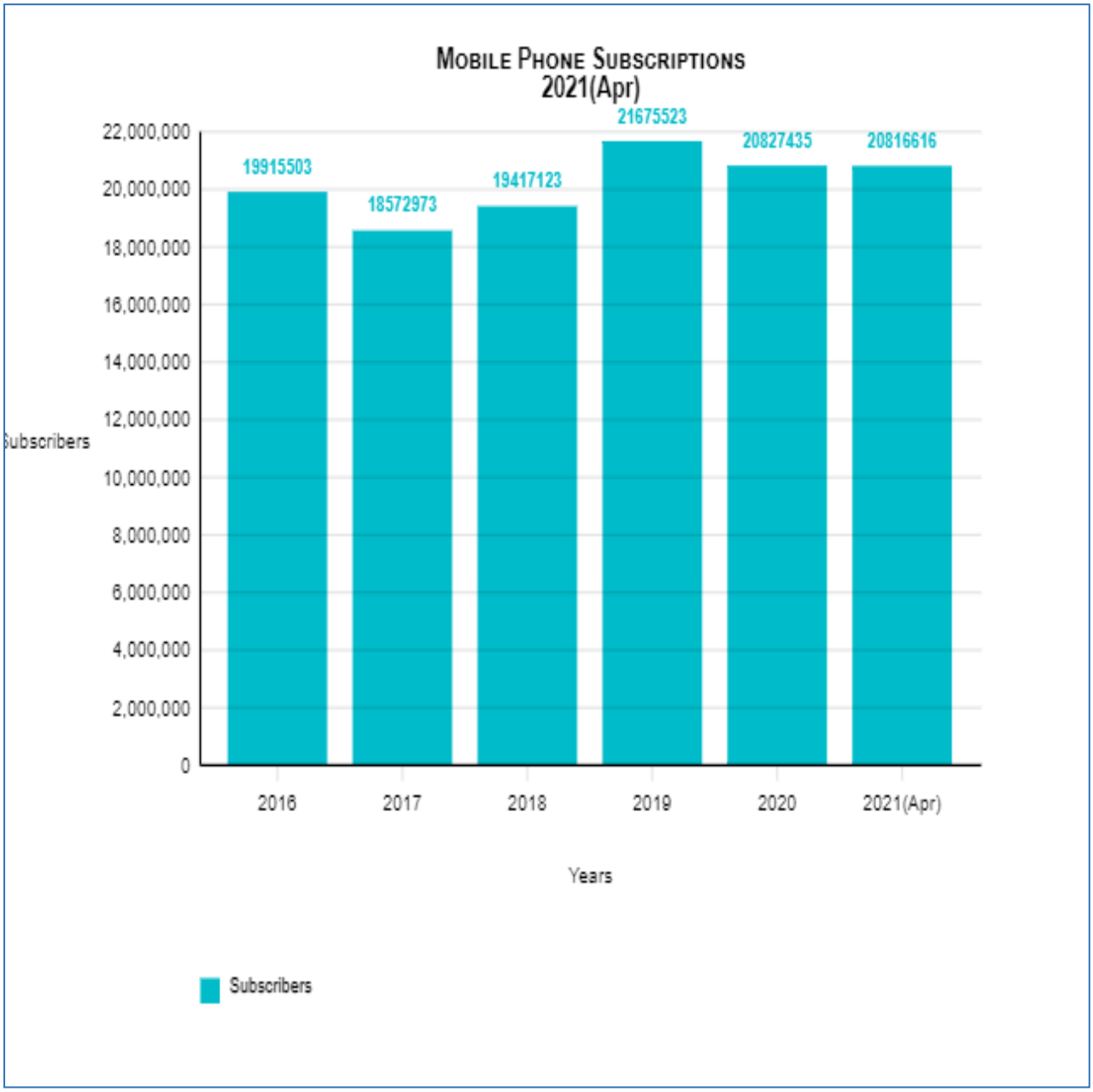
ឧបសម្ព័ន្ធទី ៥ ៖ រចនាសម្ព័ន្ធអគ្គនាយកដ្ឋានបច្ចេកវិទ្យាទូរគមនាគមន៍ និងព័ត៌មាន (ការិយាល័យ ឆ្លើយតបបន្ទាន់នៃកុំព្យូទ័រ)

ឧបសម្ព័ន្ធទី ៦ ៖ ជំពូកទី ២ បទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យា

ឧបសម្ព័ន្ធទី ១


MOBILE INTERNET
2021(Apr)
22,000,000
20,000,000
18,000,000
16,000,000
14,000,000
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
ubscribers
10649370
13611398
16126356
20340480
17808306
2017
2018
2019
2020
2021(Apr)
Years
Subscribers

ឧបសម្ព័ន្ធទី ២


Mobile Phone Subscriptions
2021(Apr)
22,000,000
20,000,000
18,000,000
16,000,000
14,000,000
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
Subscribers
19915503
18572973
19417123
21675523
20827435
20816616
2016
2017
2018
2019
2020
2021(Apr)
Years
Subscribers

ឧបសម្ព័ន្ធទី ៣

ព្រះរាជាណាចក្រកម្ពុជា
ជាតិ សាសនា ព្រះមហាក្សត្រ

សេចក្តីរាយការណ៍

ខ្ញុំបាទ/នាងខ្ញុំឈ្មោះ ..... អាយុ ..... ឆ្នាំ ..... ជនជាតិ .....
សញ្ជាតិ ..... កាន់អត្តសញ្ញាណប័ណ្ណលេខ ..... អាស័យដ្ឋាន ផ្ទះលេខ.....
ឃុំ/សង្កាត់ ..... ស្រុក/ខណ្ឌ ..... រាជធានី/ខេត្ត ..... លេខទូរស័ព្ទទំនាក់ទំនង
..... ។

សូមគោរពជូន

ឯកឧត្តម ឧត្តមសេនីយ៍ឯក ប្រធាននាយកដ្ឋានប្រឆាំងបទល្មើសបច្ចេកវិទ្យា

កម្មវត្ថុ៖.....

..... ។

តបតាមកម្មវត្ថុខាងលើ ខ្ញុំបាទ/នាងខ្ញុំ សូមជម្រាបជូន **ឯកឧត្តម ឧត្តមសេនីយ៍ឯក ប្រធាននាយកដ្ឋានប្រឆាំងបទល្មើសបច្ចេកវិទ្យា** មេត្តាជ្រាបថា៖ .....

.....

.....

.....

.....

.....

.....

.....

.....

សេចក្តីដូចបានគោរពជម្រាបជូនខាងលើ សូម **ឯកឧត្តម ឧត្តមសេនីយ៍ឯក ប្រធាននាយកដ្ឋានប្រឆាំងបទល្មើសបច្ចេកវិទ្យា** មេត្តាជ្រាបជាព័ត៌មានដ៏ខ្ពង់ខ្ពស់ ។

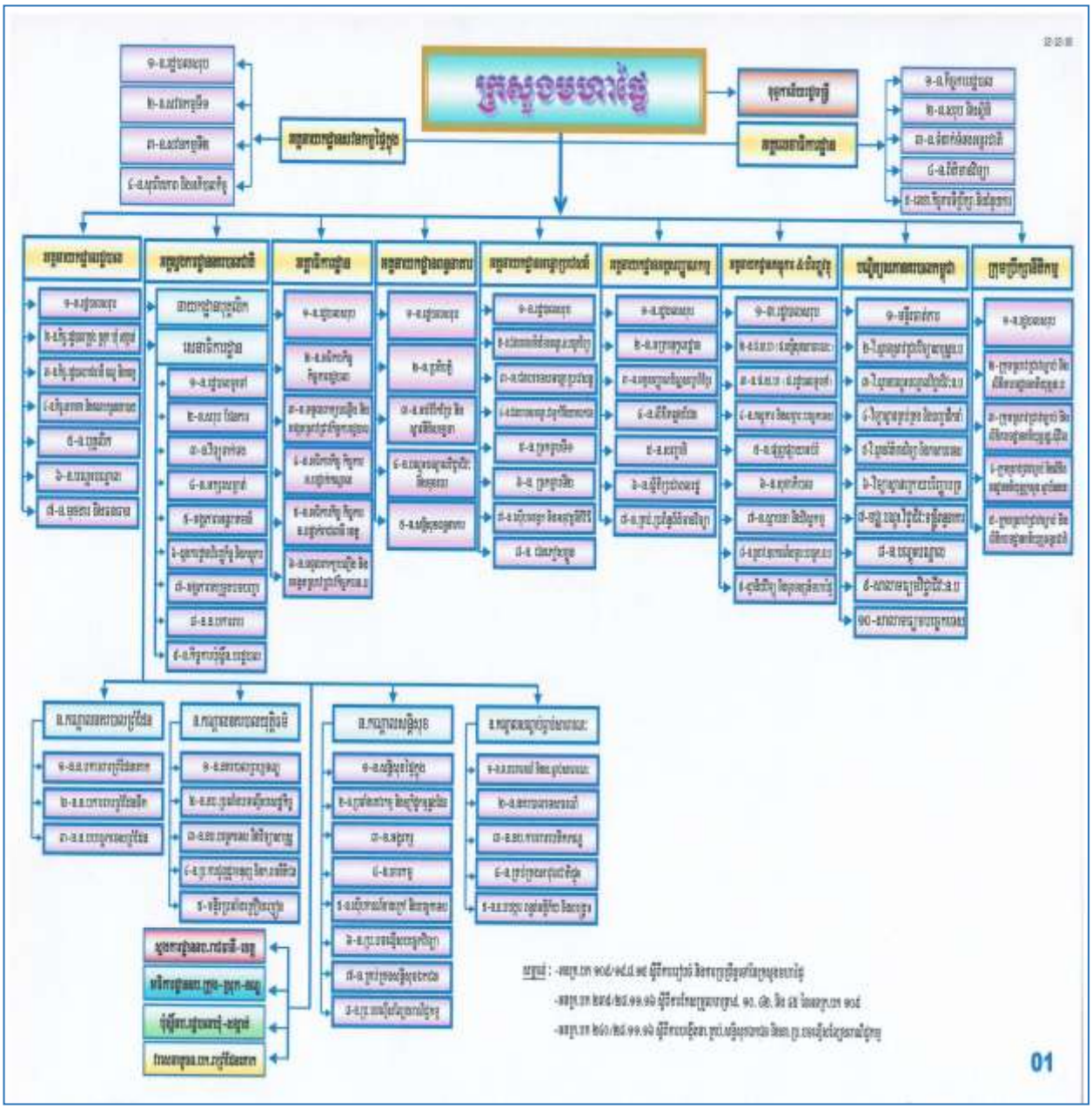
សូម **ឯកឧត្តម ឧត្តមសេនីយ៍ឯក** មេត្តា ទទួលនូវការគោរពដ៏ខ្ពង់ខ្ពស់អំពីខ្ញុំបាទ/នាងខ្ញុំ។

ថ្ងៃ ខែ ឆ្នាំជូត ទោស័ក ព.ស២៥៥៤

រាជធានីភ្នំពេញ,ថ្ងៃទី ខែ ឆ្នាំ២០២០

ស្នាមមេដៃស្តាំ

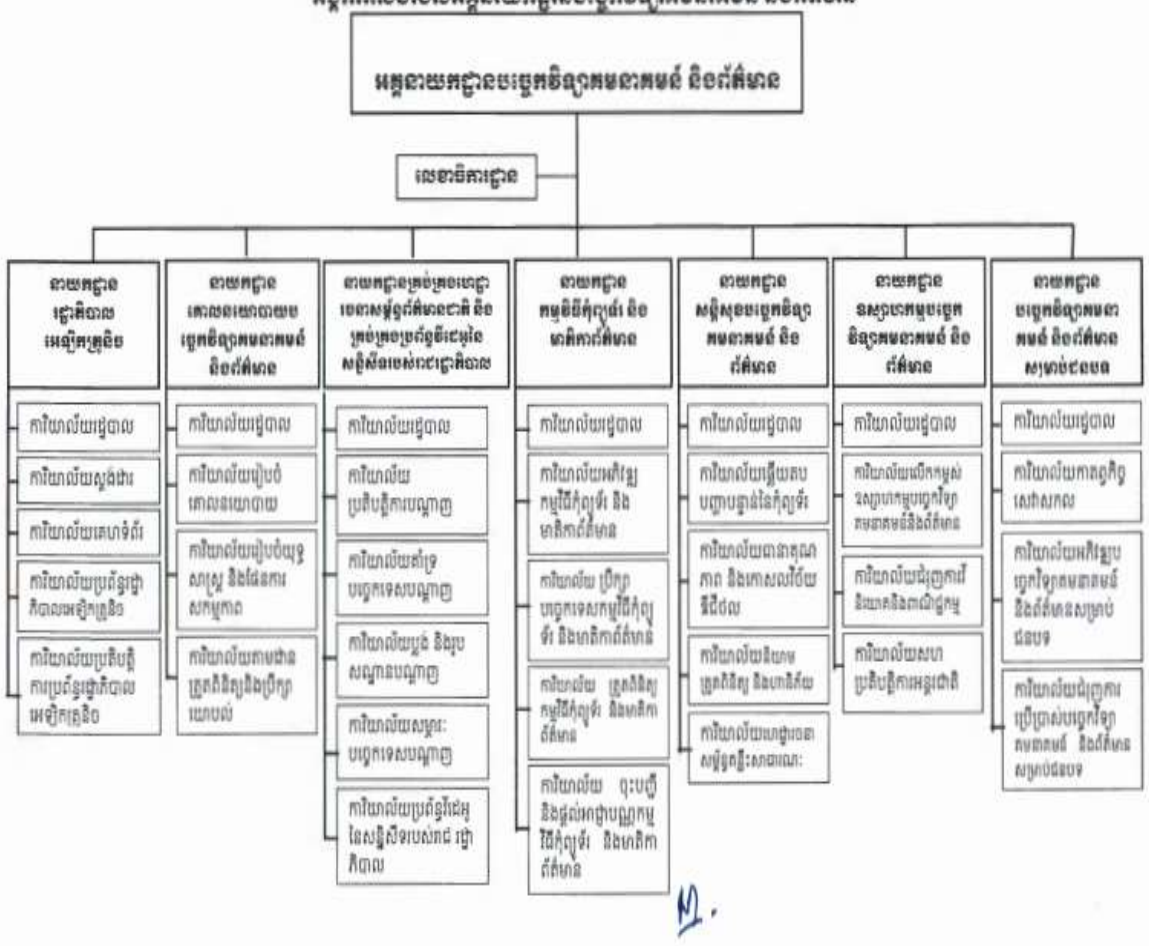
ឧបសម្ព័ន្ធទី ៤



ឧបសម្ព័ន្ធទី ៥

ឧបសម្ព័ន្ធ១ ភ្ជាប់ប្រកាសលេខ ១២៥ បទ.ប្រក ចុះថ្ងៃទី ១៦ ខែ មិថុនា ឆ្នាំ២០១៨

អង្គភាពរៀងៗខ្លួនរបស់អគ្គនាយកដ្ឋានបច្ចេកវិទ្យាគមនាគមន៍ និងព័ត៌មាន



ឧបសម្ព័ន្ធទី ៦

ជំពូកទី ២
បទល្មើសក្នុងវិស័យព័ត៌មានវិទ្យា

មាត្រា ៤២៧.- បទចូលទៅដល់ឬស្ថិតនៅនឹងប្រព័ន្ធប្រព្រឹត្តិកម្មស្ងួយប្រវត្តនៃទិន្នន័យ

អំពើចូលទៅដល់ ឬស្ថិតនៅនឹងប្រព័ន្ធប្រព្រឹត្តិកម្មស្ងួយប្រវត្តនៃទិន្នន័យ ដោយទុច្ចរិត ត្រូវផ្តន្ទាទោសដាក់ពន្ធនាគារពី ១ (មួយ) ខែ ទៅ ១ (មួយ) ឆ្នាំ និងពិន័យជាប្រាក់ពី ១០០ ០០០ (មួយសែន) រៀល ទៅ ២ ០០០ ០០០ (ពីរលាន) រៀល ។

កាលបើអំពើនោះជាហេតុបណ្តាលឱ្យមានការលុបបំបាត់ ឬកែប្រែទិន្នន័យដែលមាននៅក្នុងប្រព័ន្ធ ឬឱ្យមានការខូចខាតនូវដំណើរការនៃប្រព័ន្ធ បទល្មើសនេះត្រូវផ្តន្ទាទោសដាក់ពន្ធនាគារពី ១ (មួយ) ឆ្នាំ ទៅ ២ (ពីរ) ឆ្នាំ និងពិន័យជាប្រាក់ពី ២ ០០០ ០០០ (ពីរលាន) រៀល ទៅ ៤ ០០០ ០០០ (បួនលាន) រៀល ។

មាត្រា ៤២៨.- បទបង្កើតជាឧបសគ្គដល់ដំណើរការនៃប្រព័ន្ធប្រព្រឹត្តិកម្មស្ងួយប្រវត្តនៃទិន្នន័យ

អំពើបង្កើតជាឧបសគ្គ ធ្វើឱ្យខូចដំណើរការនៃប្រព័ន្ធប្រព្រឹត្តិកម្មស្ងួយប្រវត្តនៃទិន្នន័យ ត្រូវផ្តន្ទាទោសដាក់ពន្ធនាគារពី ១ (មួយ) ឆ្នាំ ទៅ ២ (ពីរ) ឆ្នាំ និងពិន័យជាប្រាក់ពី ២ ០០០ ០០០ (ពីរលាន) រៀល ទៅ ៤ ០០០ ០០០ (បួនលាន) រៀល ។

មាត្រា ៤២៩.- បទបញ្ចូល លុបបំបាត់ ឬកែប្រែដោយទុច្ចរិតនូវទិន្នន័យ

អំពើបញ្ចូល លុបបំបាត់ ឬកែប្រែដោយទុច្ចរិតនូវទិន្នន័យទៅក្នុងប្រព័ន្ធប្រព្រឹត្តិកម្មស្ងួយប្រវត្ត ត្រូវផ្តន្ទាទោសដាក់ពន្ធនាគារពី ១ (មួយ) ឆ្នាំ ទៅ ២ (ពីរ) ឆ្នាំ និងពិន័យជាប្រាក់ពី ២ ០០០ ០០០ (ពីរលាន) រៀល ទៅ ៤ ០០០ ០០០ (បួនលាន) រៀល ។

មាត្រា ៤៣០.- បទចូលរួមក្នុងក្រុមប្រមូលផ្តុំ ឬក្នុងសន្និដ្ឋានការដើម្បីរៀបចំប្រព្រឹត្តបទល្មើស

អំពើចូលរួមទៅក្នុងក្រុមប្រមូលផ្តុំ ឬទៅក្នុងសន្និដ្ឋានការ ដែលបង្កើតឡើងដើម្បីរៀបចំប្រព្រឹត្តបទល្មើសដែលមានចែងក្នុងផ្នែកនេះ ត្រូវផ្តន្ទាទោសដាក់ពន្ធនាគារពី ១

(មួយ) ឆ្នាំ ទៅ ២ (ពីរ) ឆ្នាំ និងពិន័យជាប្រាក់ពី ២ ០០០ ០០០ (ពីរលាន) រៀល ទៅ ៤ ០០០ ០០០ (បួនលាន) រៀល ។

មាត្រា ៤៣១.- ការប៉ុនប៉ង

ការប៉ុនប៉ងប្រព្រឹត្តបទមជ្ឈិមដែលមានចែងក្នុងផ្នែកនេះ ត្រូវផ្តន្ទាទោសដូចគ្នានឹងបទមជ្ឈិមខាងលើដែរ ។

មាត្រា ៤៣២.- ទោសបន្ថែម : ប្រភេទ និងរយៈពេល

ចំពោះបទមជ្ឈិមដែលមានចែងក្នុងផ្នែកនេះ ទោសបន្ថែមដូចតទៅនេះ អាចត្រូវបានប្រកាស :

១-ការដកសិទ្ធិខ្លះជាពលរដ្ឋ ជាស្ថាពរ ឬសម្រាប់រយៈពេល ៥ (ប្រាំ) ឆ្នាំ យ៉ាងច្រើន ។

២-ការហាមឃាត់ចំពោះការប្រកបវិជ្ជាជីវៈ កាលបើបទល្មើសនេះបានប្រព្រឹត្តនៅក្នុងការប្រកបវិជ្ជាជីវៈ ឬនៅក្នុងនិកាសនៃការប្រកបវិជ្ជាជីវៈនេះ ជាស្ថាពរ ឬសម្រាប់រយៈពេល ៥ (ប្រាំ) ឆ្នាំ យ៉ាងច្រើន ។

៣-ការរឹបអូសនូបករណ៍ សម្ភារៈ ឬវត្ថុណាមួយ ដែលប្រើប្រាស់សម្រាប់ប្រព្រឹត្តបទល្មើស ឬដែលមានគោលដៅប្រព្រឹត្តបទល្មើស ។

៤-ការរឹបអូសវត្ថុ ឬមូលនិធិ ដែលជាកម្មវត្ថុនៃបទល្មើស ។

៥-ការរឹបអូសផលទុន និងទ្រព្យសម្បត្តិដែលជាផលកើតចេញពីបទល្មើស ។

៦-ការរឹបអូសនូបភោគភណ្ឌ សម្ភារៈ ឬចលនវត្ថុនៅក្នុងទីកន្លែងដែលបទល្មើសនោះបានប្រព្រឹត្ត ។

៧-ការរឹបអូសយានជំនិះរបស់ទណ្ឌិតមួយគ្រឿង ឬច្រើនគ្រឿង ។

៨-ការបិទផ្សាយសេចក្តីសម្រេចផ្តន្ទាទោស សម្រាប់រយៈពេល ២ (ពីរ) ខែ យ៉ាងច្រើន ។

៩-ការផ្សាយសេចក្តីសម្រេចផ្តន្ទាទោសនៅក្នុងសារព័ត៌មាន ។

១០-ការផ្សាយសេចក្តីសម្រេចផ្តន្ទាទោស តាមគ្រប់មធ្យោបាយទូរគមនាគមន៍សោតទស្សន៍ សម្រាប់រយៈពេល ៨ (ប្រាំបី) ថ្ងៃ យ៉ាងច្រើន ។