പതിനാറാം കേരളനിയമസഭ

രണ്ടാം സമ്മേളനം

നക്ഷത്രചിഹ്നമിടാത്ത ചോദ്യം നമ്പർ: 2222 **27-10-2026-ൽ മറുപടിയ്ക്ക്**

സൈബർ സുരക്ഷ

ചോദ്യം ഉന്നയിച്ച അംഗങ്ങൾ

ശ്രീ. ഷിബു തെക്കുംപുറം

ശ്രീ. അപു ജോൺ ജോസഫ്

ശ്രീ. വിനു ജോബ് കുഴിമണ്ണിൽ

മറുപടി നൽകിയ മന്ത്രി

ശ്രീ. രമേശ് ചെന്നിത്തല

(ആഭ്യന്തര- വിജിലൻസ്, കയർ വകുപ്പ് മന്ത്രി)

(എ) സംസ്ഥാനത്ത് സൈബർ സുരക്ഷയ്ക്കായി വകുപ്പ് ഒരുക്കിയിട്ടുള്ള സംവിധാനങ്ങൾ വിശദമാക്കാമോ;

മറുപടി: സംസ്ഥാനത്ത് സൈബർ കുറ്റകൃത്യങ്ങൾ തടയുന്നതിനും അന്വേഷിക്കുന്നതിനും പൊതുജനങ്ങളുടെ ഡിജിറ്റൽ സുരക്ഷ ഉറപ്പാക്കുന്നതിനുമായി കേരള പോലീസ് വിവിധ സാങ്കേതിക, അന്വേഷണ, പരിശീലന സംവിധാനങ്ങൾ ഏർപ്പെടുത്തിയിട്ടുണ്ട്. പരാതികൾ സ്വീകരിക്കുന്നതിനും കേസുകൾ രജിസ്റ്റർ ചെയ്ത് അന്വേഷണം നടത്തുന്നതിനുമായി സംസ്ഥാനത്തെ 20 പോലീസ് ജില്ലകളിലും സൈബർ പോലീസ് സ്റ്റേഷനുകൾ പ്രവർത്തിച്ചു വരുന്നു. സൈബർ ഓപ്പറേഷൻസിന്റെ കീഴിൽ പബ്ലിക് ഔട്ട്റീച്ച് ഗ്രൂപ്പ്, സൈബർ ഫ്രോഡ് ആൻഡ് സോഷ്യൽ മീഡിയ ഗ്രൂപ്പ്, സൈബർ സെക്യൂരിറ്റി ആൻഡ് അഡ്വാൻസ്ഡ് ക്രൈം ഗ്രൂപ്പ്, സൈബർ ഡോമുകൾ, അനാലിസിസ് വിംഗ്, ട്രെയിനിങ് ആൻഡ് കപ്പാസിറ്റി ബിൽഡിംഗ് വിഭാഗം എന്നിവയും പ്രവർത്തിച്ചു വരുന്നു.

വർദ്ധിച്ചു വരുന്ന സൈബർ കുറ്റകൃത്യങ്ങളെ നേരിടുന്നതിനും അവയെ വിശകലനം ചെയ്ത് കുറ്റകൃത്യങ്ങൾക്ക് ഇടയാക്കുന്ന വസ്തുതകൾ കണ്ടെത്തി ഇല്ലായ്മ ചെയ്യുന്നതിന് സൈബർ ഡിവിഷൻ പരിശ്രമിക്കുകയും സൈബർ കുറ്റകൃത്യങ്ങളുമായി ബന്ധപ്പെട്ട അന്വേഷണങ്ങളിൽ പോലീസ് സ്റ്റേഷനുകൾക്കും സൈബർ സെല്ലുകൾക്കും ആവശ്യമായ സാങ്കേതിക സഹായം നൽകുകയും ചെയ്യുന്നു.

ഓൺലൈൻ സാമ്പത്തിക തട്ടിപ്പിനിരയാകുന്നവർക്ക് പരാതികൾ രജിസ്റ്റർ ചെയ്യുന്നതിനായി NCRP (National Cyber Crime Reporting Portal) മുഖേനയും 1930 എന്ന ടോൾഫ്രീ ഹെൽപ്ലൈൻ നമ്പർ മുഖേനയും സൗകര്യം ഏർപ്പെടുത്തിയിട്ടുണ്ട്. ഇതിനായി 24 മണിക്കൂറും പ്രവർത്തിക്കുന്ന കോൾ സെന്ററും സജ്ജീകരിച്ചിട്ടുണ്ട്. ബാങ്കുകളുമായി ഏകോപനം നടത്തി തട്ടിപ്പിലൂടെ നഷ്ടപ്പെട്ട തുകയുടെ തുടർ കൈമാറ്റം തടയുന്നതിനും ലഭ്യമായ സാഹചര്യങ്ങളിൽ തുക തിരിച്ചുപിടിക്കുന്നതിനും നടപടികൾ സ്വീകരിച്ചു വരുന്നു. കൂടാതെ, തട്ടിപ്പിനായി ഉപയോഗിക്കുന്ന മൊബൈൽ സിം കാർഡുകൾ, ഉപകരണങ്ങളുടെ IMEI നമ്പറുകൾ, മ്യൂൾ അക്കൗണ്ടുകൾ (Mule Accounts) എന്നിവ തിരിച്ചറിഞ്ഞ് ബ്ലോക്ക് ചെയ്യുന്നതിനും മരവിപ്പിക്കുന്നതിനും ബന്ധപ്പെട്ട ഏജൻസികളുമായി ഏകോപനം നടത്തി നടപടികൾ സ്വീകരിച്ചു വരുന്നു.

കേരള പോലീസിന്റെ സൈബർ ഓപ്പറേഷൻസ് വിഭാഗത്തിന്റെ നേതൃത്വത്തിൽ സൈബർ സാമ്പത്തിക തട്ടിപ്പുകൾ റിപ്പോർട്ട് ചെയ്യുന്നതിനും തട്ടിപ്പിലൂടെ നഷ്ടപ്പെട്ട തുകയുടെ തുടർ കൈമാറ്റം തടയുന്നതിനും ആവശ്യമായ നടപടികൾ സ്വീകരിച്ചു വരുന്നു. തട്ടിപ്പിനിരയാകുന്നവർക്ക് 1930 എന്ന ടോൾഫ്രീ ഹെൽപ്ലൈൻ നമ്പർ മുഖേനയും നാഷണൽ സൈബർ ക്രൈം റിപ്പോർട്ടിംഗ് പോർട്ടലായ (NCRP) www.cybercrime.gov.in മുഖേനയും പരാതി രജിസ്റ്റർ ചെയ്യാവുന്നതാണ്. പരാതി ലഭിക്കുന്ന മുറയ്ക്ക് ബന്ധപ്പെട്ട ബാങ്കുകളുമായി ഏകോപനം നടത്തി ഇടപാട് വിവരങ്ങൾ ശേഖരിക്കുകയും നഷ്ടപ്പെട്ട തുക തടഞ്ഞുവയ്ക്കുന്നതിനും ലഭ്യമായ സാഹചര്യങ്ങളിൽ തിരിച്ചുപിടിക്കുന്നതിനും ആവശ്യമായ നടപടികൾ സ്വീകരിക്കുകയും ചെയ്യുന്നു. തട്ടിപ്പുമായി ബന്ധപ്പെട്ട ബാങ്ക് അക്കൗണ്ട് വിവരങ്ങളും ഇടപാടുകളുടെ വിശദാംശങ്ങളും ശേഖരിച്ച് അന്വേഷണ ഉദ്യോഗസ്ഥർക്ക് കൈമാറുകയും പരാതിക്കാരിൽ നിന്ന് കൂടുതൽ വിവരങ്ങൾ ശേഖരിച്ച് തുടർനടപടികൾ സ്വീകരിക്കുകയും ചെയ്യുന്നു.

സൈബർ സാമ്പത്തിക തട്ടിപ്പുകളെക്കുറിച്ച് പൊതുജനങ്ങളിൽ അവബോധം സൃഷ്ടിക്കുന്നതിനായി ബോധവൽക്കരണ ക്ലാസുകൾ, വീഡിയോകൾ, പോസ്റ്ററുകൾ, ഓൺലൈൻ പരിപാടികൾ എന്നിവ സംഘടിപ്പിച്ചു വരുന്നു. മുതിർന്ന പൗരന്മാർ ഉൾപ്പെടെയുള്ള വിഭാഗങ്ങളെ ലക്ഷ്യമിട്ട് പ്രത്യേക ബോധവൽക്കരണ സന്ദേശങ്ങളും തയ്യാറാക്കി കേരള പോലീസിന്റെ ഔദ്യോഗിക സാമൂഹ്യമാധ്യമങ്ങൾ, കേരള പോലീസ് മീഡിയ സെന്റർ, റസിഡന്റ്സ് അസോസിയേഷനുകൾ, മറ്റ് സംഘടനകൾ എന്നിവ മുഖേന പ്രചരിപ്പിക്കുന്നുണ്ട്.

കൂടാതെ, സൈബർ സാമ്പത്തിക തട്ടിപ്പുകളുടെ രീതികളും പ്രവണതകളും വിശകലനം ചെയ്ത് അവ തടയുന്നതിനും കുറ്റവാളികളെ കണ്ടെത്തുന്നതിനും നടപടികൾ സ്വീകരിച്ചു വരുന്നു. ഇതിന്റെ ഭാഗമായി ഓപ്പറേഷൻ CY HUNT ഉൾപ്പെടെയുള്ള നടപടികളിലൂടെ സൈബർ കുറ്റവാളികളെയും തട്ടിപ്പിനായി ഉപയോഗിക്കുന്ന ബാങ്ക് അക്കൗണ്ടുകൾ നൽകുന്നവരെയും കണ്ടെത്തി നിയമനടപടികൾ സ്വീകരിക്കുന്നു.

സൈബർ സാമ്പത്തിക തട്ടിപ്പുകളുമായി ബന്ധപ്പെട്ട ബാങ്ക് അക്കൗണ്ടുകൾ, മൊബൈൽ നമ്പറുകൾ, ഉപകരണങ്ങൾ എന്നിവ പരിശോധിച്ച് തട്ടിപ്പിനായി ഉപയോഗിക്കുന്ന മ്യൂൾ അക്കൗണ്ടുകൾ (Mule Accounts) മരവിപ്പിക്കുന്നതിനും ബന്ധപ്പെട്ട മൊബൈൽ നമ്പറുകളും ഉപകരണങ്ങളും ബ്ലോക്ക് ചെയ്യുന്നതിനും ബാങ്കുകളുമായും ടെലികോം സേവനദാതാക്കളുമായും ഏകോപനം നടത്തി നടപടികൾ സ്വീകരിച്ചു വരുന്നു.

സൈബർ സാമ്പത്തിക തട്ടിപ്പുകൾ സംബന്ധിച്ച പരാതികളിൽ സമയബന്ധിതമായി നടപടി സ്വീകരിക്കുന്നതിനായി നാഷണൽ സൈബർ ക്രൈം റിപ്പോർട്ടിംഗ് പോർട്ടലായ (NCRP) സംവിധാനവും ബാങ്കുകളുടെയും ടെലികോം സേവനദാതാക്കളുടെയും സംവിധാനങ്ങളും സംയോജിപ്പിച്ചിട്ടുണ്ട്. കൂടാതെ, കേരള പോലീസ് ആസ്ഥാനത്ത് പ്രവർത്തിക്കുന്ന ജോയിന്റ് സൈബർ കോർഡിനേഷൻ സെന്റർ (JCCT) മുഖേന ബാങ്കുകളുമായി ഏകോപനം നടത്തി ഇടപാട് വിവരങ്ങൾ ശേഖരിക്കുന്നതിനും തട്ടിപ്പിലൂടെ കൈമാറ്റം ചെയ്യപ്പെടുന്ന തുക തടഞ്ഞു വയ്ക്കുന്നതിനും നടപടികൾ സ്വീകരിക്കുന്നു. അഞ്ച് ലക്ഷം രൂപയ്ക്ക് മുകളിലുള്ള സൈബർ സാമ്പത്തിക തട്ടിപ്പ് പരാതികളിൽ എഫ്.ഐ.ആർ. രജിസ്ട്രേഷൻ വേഗത്തിലാക്കുന്നതിനായി ഇ-സീറോ എഫ്.ഐ.ആർ. (e-Zero FIR) സംവിധാനവും കേരള പോലീസിന്റെ ICOPS (Integrated Core Policing System)പ്ലാറ്റ്ഫോമുമായി സംയോജിപ്പിച്ച് നടപ്പിലാക്കിയിട്ടുണ്ട്.

സൈബർ പട്രോളിങ്ങിലൂടെ തട്ടിപ്പിനായി ഉപയോഗിക്കുന്ന വെബ്സൈറ്റുകൾ, അനധികൃത ഓൺലൈൻ ലോൺ ആപ്പുകൾ, സാമൂഹ്യമാധ്യമ അക്കൗണ്ടുകൾ, പോസ്റ്റുകൾ, പേജുകൾ എന്നിവ കണ്ടെത്തി നിർജീവമാക്കുന്നതിനുള്ള നടപടികൾ സൈബർ ആസ്ഥാനത്തെ സൈബർ ഫ്രോഡ് ആൻഡ് സോഷ്യൽ മീഡിയ ഗ്രൂപ്പ് സ്വീകരിച്ചു വരുന്നു.

കേരള പോലീസിന്റെ കമ്പ്യൂട്ടറുകളുടെയും നെറ്റ്‌വർക്കുകളുടെയും സുരക്ഷ ഉറപ്പാക്കുന്നതിനായി സൈബർ സെക്യൂരിറ്റി ആൻഡ് അഡ്വാൻസ്ഡ് ക്രൈം വിഭാഗം പ്രവർത്തിക്കുന്നു. BSNL, കൊച്ചിൻ യൂണിവേഴ്സിറ്റി ഓഫ് സയൻസ് ആൻഡ് ടെക്നോളജി(CUSAT), ഇന്ത്യൻ ഇൻസ്റ്റ്യൂട്ട് ഓഫ് ഇൻഫർമേഷൻ ടെക്നോളജി (IIT), നാഷണൽ ഫോറൻസിക് സയൻസ് യൂണിവേഴ്സിറ്റി (NFSU) എന്നീ സ്ഥാപനങ്ങളുമായി സഹകരിച്ച് പോലീസ് ഉദ്യോഗസ്ഥർക്ക് സൈബർ ആക്രമണങ്ങൾ നേരിടുന്നതിനുള്ള പരിശീലനം നൽകുകയും എല്ലാ ജില്ലകളിലും ഇൻസിഡന്റ് റെസ്പോൺസ് ടീമുകൾ രൂപീകരിക്കുകയും ചെയ്തിട്ടുണ്ട്. ഈ ടീമുകളുടെ സഹായത്തോടെ 13 സൈബർ ആക്രമണങ്ങൾ തടയുകയും വിവിധ സർക്കാർ വകുപ്പുകളിലെ 31 ഡാറ്റാ ബ്രീച്ചുകൾ ഡാർക്ക് വെബ് അന്വേഷണത്തിലൂടെ കണ്ടെത്തി ബന്ധപ്പെട്ട വകുപ്പുകളെ അറിയിക്കുകയും ചെയ്തിട്ടുണ്ട്. സൈബർ ആക്രമണങ്ങൾ മുൻകൂട്ടി തിരിച്ചറിഞ്ഞ് തടയുന്നതിനായി സൈബർ ഡോമും പ്രവർത്തിച്ചു വരുന്നു.

കുട്ടികൾക്കെതിരായ ഓൺലൈൻ ലൈംഗിക ചൂഷണം തടയുന്നതിനായി കൗണ്ടർ ചൈൽഡ് സെക്ഷ്വൽ എക്സ്പ്ലോയിറ്റേഷൻ സെന്റർ (Counter Child Sexual Exploitation Centre)പ്രവർത്തിക്കുന്നു. ഓപ്പറേഷൻ പി-ഹണ്ട് മുഖേന നിരവധി കുറ്റവാളികളെ അറസ്റ്റ് ചെയ്യുകയും കേസുകൾ രജിസ്റ്റർ ചെയ്ത് കുറ്റകൃത്യങ്ങൾക്ക് ഉപയോഗിച്ച ഉപകരണങ്ങൾ പിടിച്ചെടുക്കുകയും ചെയ്തിട്ടുണ്ട്.

കൂടാതെ, ടെയിനിങ് ആൻഡ് കപ്പാസിറ്റി ബിൽഡിംഗ് വിഭാഗം മുഖേന വിവിധ റാങ്കുകളിലുള്ള പോലീസ് ഉദ്യോഗസ്ഥർക്ക് സൈബർ കുറ്റകൃത്യങ്ങൾ സംബന്ധിച്ച പരിശീലനം നൽകുകയും പൊതുജനങ്ങൾക്കായി ബോധവൽക്കരണ പരിപാടികൾ സംഘടിപ്പിക്കുകയും ചെയ്യുന്നു. നാല് റേഞ്ച് ഡി.ഐ.ജി.മാരുടെ കീഴിൽ സൈബർ കുറ്റാന്വേഷണങ്ങൾ ഏകോപിപ്പിക്കുന്നതിനും വിവരശേഖരണത്തിനുമായി സൈബർ പട്രോളിങ് വിഭാഗവും പ്രവർത്തിച്ചു വരുന്നു

(ബി) കേരള പോലീസിന്റെ സൈബർ ഡോമിന്റെ പ്രവർത്തനം വ്യക്തമാക്കാമോ;

<u>മറുപടി:</u> സൈബർ കുറ്റകൃത്യങ്ങൾ പ്രതിരോധിക്കുന്നതിനും മേഖലയിലെ നൂതന സാങ്കേതികവിദ്യകൾ വികസിപ്പിച്ച് പ്രയോഗിക്കുന്നതിനുമായി കേരള പോലീസിന്റെ കീഴിൽ പ്രവർത്തിക്കുന്ന ഗവേഷണ-വിശകലന വിഭാഗമാണ് സൈബർഡോം (Cyberdome). സൈബർ സുരക്ഷാ വിദഗ്ധർ, സാങ്കേതിക മേഖലകളിലെ വോളന്റിയർമാർ, ഗവേഷകർ, വ്യവസായ പങ്കാളികൾ എന്നിവരുടെ സജീവ പങ്കാളിത്തത്തോടെ പബ്ലിക്-പ്രൈവറ്റ് പാർട്ണർഷിപ്പ് (PPP) മാതൃകയിൽ പ്രവർത്തിക്കുന്ന സൈബർഡോം, സാങ്കേതിക വൈദഗ്ധ്യവും നൂതന ആശയങ്ങളും പോലീസിംഗുമായി സംയോജിപ്പിച്ച് സൈബർ കുറ്റകൃത്യങ്ങൾക്കെതിരായ പ്രതിരോധ സംവിധാനങ്ങൾ ശക്തിപ്പെടുത്തുന്നതിൽ പങ്കു വഹിക്കുന്നു. നിർണായക സൈബർ സുരക്ഷാ മേഖലയിലെ സാങ്കേതിക നവീകരണം, വിജ്ഞാന കൈമാറ്റം, ശേഷിവികസനം എന്നിവയ്ക്ക് പ്രത്യേക പ്രാധാന്യം നൽകുന്ന സൈബർഡോം, സർക്കാർ, അർധസർക്കാർ വിദ്യാഭ്യാസ സ്ഥാപനങ്ങളിലെ സാങ്കേതിക വിഭാഗങ്ങളുമായി സഹകരിച്ച് സൈബർ സുരക്ഷാ വർക്ക്ഷോപ്പുകൾ, സെമിനാറുകൾ, പരിശീലന പരിപാടികൾ എന്നിവ സംഘടിപ്പിച്ചു വരുന്നു. കാര്യക്ഷമമായ പോലീസിംഗിനായി നൂതന സാങ്കേതികവിദ്യകളുടെ പ്രയോഗം പ്രോത്സാഹിപ്പിക്കുന്നതിനൊപ്പം, പൊതുജനങ്ങൾ, അർധസർക്കാർ സ്ഥാപനങ്ങൾ, വിദ്യാഭ്യാസ സ്ഥാപനങ്ങൾ എന്നിവയുടെ സൈബർ സുരക്ഷാ അവബോധവും സാങ്കേതിക ശേഷിയും വർധിപ്പിക്കുന്നതിനും സൈബർഡോം പ്രത്യേക ശ്രദ്ധ നൽകുന്നു.

നൂതന സാങ്കേതികവിദ്യ, ഗവേഷണം, വിദഗ്ധ സഹകരണം, പ്രതിരോധാധിഷ്ഠിത സൈബർ സുരക്ഷാ തന്ത്രങ്ങൾ എന്നിവ സംയോജിപ്പിച്ച് സുരക്ഷിതമായ ഡിജിറ്റൽ അന്തരീക്ഷം സൃഷ്ടിക്കുകയും സാങ്കേതികവിദ്യാധിഷ്ഠിതമായ കാര്യക്ഷമമായ പോലീസിംഗ് ശക്തിപ്പെടുത്തുകയും ചെയ്യുക എന്നതാണ് സൈബർഡോമിന്റെ പ്രവർത്തനങ്ങളുടെ പ്രധാന ലക്ഷ്യം. സെക്യൂരിറ്റി ഓപ്പറേഷൻസ്

സെന്റർ (SOC), ഡാർക്ക് വെബ് മോണിറ്ററിങ് ആൻഡ് ഇൻവെസ്റ്റിഗേഷൻ, KidGlove പദ്ധതി, HACKP, സൈബർ സെക്യൂരിറ്റി ട്രെയിനിങ് ആൻഡ് കപ്പാസിറ്റി ബിൽഡിങ് എന്നിവ ഇതിലെ പ്രധാന പ്രവർത്തനങ്ങളാണ്.

1. Security Operations Centre (SOC)

കേരള പോലീസിന്റെ ഐ.ടി. സംവിധാനങ്ങളിലെ സൈബർ സുരക്ഷാ നിരീക്ഷണം, സൈബർ ഭീഷണികളുടെ കണ്ടെത്തൽ, വിശകലനം, പ്രതികരണം എന്നിവയ്ക്കായി AI-enabled SOC പ്രവർത്തിക്കുന്നു.

2. Dark Web Intelligence

ഡാർക്ക് വെബിൽ നടക്കുന്ന നിയമവിരുദ്ധ പ്രവർത്തനങ്ങളും സൈബർ ഭീഷണികളും നിരീക്ഷിച്ച് ആവശ്യമായ വിവരങ്ങൾ ശേഖരിക്കുകയും ബന്ധപ്പെട്ട അധികാരികൾക്ക് കൈമാറുകയും ചെയ്യുന്നു.

3. KidGlove പദ്ധതി

കുട്ടികളെയും രക്ഷിതാക്കളെയും അധ്യാപകരെയും സുരക്ഷാ പോലീസുദ്യോഗസ്ഥരെയും ലക്ഷ്യമിട്ട് സൈബർ ബോധവൽക്കരണവും ഓൺലൈൻ സുരക്ഷാ പരിശീലനവും നൽകുന്നു.

4. Cyber Security Awareness Programmes

സൈബർ തട്ടിപ്പുകൾ, ഓൺലൈൻ സാമ്പത്തിക തട്ടിപ്പുകൾ, സോഷ്യൽ മീഡിയ ദുരുപയോഗം തുടങ്ങിയവ സംബന്ധിച്ച് പൊതുജനങ്ങൾക്കും വിവിധ വിഭാഗങ്ങൾക്കും ബോധവൽക്കരണ പരിപാടികൾ സംഘടിപ്പിക്കുന്നു.

5. HACKP National Cyber Security Hackathon

സൈബർ കുറ്റകൃത്യങ്ങളുടെ അന്വേഷണത്തിനും സൈബർ സുരക്ഷയ്ക്കും സഹായകരമായ നൂതന സാങ്കേതിക പരിഹാരങ്ങൾ വികസിപ്പിക്കുന്നതിനായി ഹാക്കത്തോൺ സംഘടിപ്പിക്കുന്നു.

6. Cyber Security Training & Capacity Building

പോലീസ് ഉദ്യോഗസ്ഥർക്ക് സൈബർ കുറ്റാന്വേഷണം, ഡിജിറ്റൽ തെളിവുകളുടെ കൈകാര്യം, സൈബർ സുരക്ഷ തുടങ്ങിയ മേഖലകളിൽ പരിശീലനം നൽകുകയും സാങ്കേതിക ശേഷി വർദ്ധിപ്പിക്കുകയും ചെയ്യുന്നു.

(സി) സൈബർ സുരക്ഷാ പ്രവർത്തനങ്ങൾ കൂടുതൽ കാര്യക്ഷമമാക്കുന്നതിനായി ക്വാണ്ടം കമ്പ്യൂട്ടിങ്, റോബോട്ടിക്സ് മേഖലകളിൽ പുതിയ സാങ്കേതിക വിദ്യകൾ ഉപയോഗപ്പെടുത്താൻ ഈ രംഗത്തെ ഉന്നത വിദ്യാഭ്യാസ സ്ഥാപനങ്ങളുമായി സഹകരിക്കാൻ പദ്ധതിയുണ്ടോ; വ്യക്തമാക്കാമോ?

<u>മറുപടി:</u> ക്വാണ്ടം കമ്പ്യൂട്ടിംഗ്, സൈബർ സെക്യൂരിറ്റി, റോബോട്ടിക്സ് തുടങ്ങിയ മേഖലകളിൽ സഹകരിച്ച് പ്രവർത്തിക്കുന്നതിനായി കേരള പോലീസ് സൈബർ ഡോമും അലയൻസ് സർവകലാശാലയും ധാരണപത്രം ഒപ്പുവച്ചിട്ടുണ്ട്. കൂടാതെ റോബോട്ടിക്സ് മേഖലയിൽ പ്രാവീണ്യമുള്ള വോളന്റിയർമാരെ കണ്ടെത്തി, ഈ മേഖലയിലെ പുതിയ സാങ്കേതിക വിദ്യയും നൂനത ആശയങ്ങളും ഉപയോഗപ്പെടുത്താനുള്ള പ്രാരംഭനടപടികൾ ആവിഷ്കരിച്ചു വരുന്നു.

സെക്ഷൻ ഓഫീസർ