Európai (Visegrádi országok) kiberbiztonsága javaslat az az ázsiai országok részére: Vietnam ügye

Nguyen Huu Phuoc Dai

Témavezető: ***Prof.Dr. Rajnai Zoltán***

1. Bevezetés

A számítógépes bűncselekmények manapság bonyolultabbak, és így hatalmas károkat vagy befolyást jelentenek a szervezetekre, az egyénekre és a nemzetbiztonságra. Ezért a számítógép és a hálózat biztonsága nemcsak a hagyományos biztonsági tudatosító szervezetekre vonatkozik; például katonai, banki vagy pénzügyi intézményekre, hanem minden egyes számítógépet használó egyéni és kormányzati tisztviselő számára. Vietnam, ez a délkelet-ázsiai kis ország, szintén a világ 20 legnépesebb országának egyike, Vietnamban az információs és kommunikációs technológia (IKT) iparág nemrégiben fejlődött ki. A késői kezdet ellenére Vietnam gyorsan megközelítette a világ modern távközlési infrastruktúráját, de Vietnam kormánya nem figyelt a hálózati biztonságra vagy a számítógépes fenyegetések okozta károkra. Ebből következően a dolgozat célja annak vizsgálata, hogy Vietnam készen áll-e a biztonsági problémákra, vagy milyen megoldást találna rájuk. Az értekezés a következő hat fontos kérdés megválaszolására törekszik:

- Mik azok a számítógépes fenyegetések?
- Veszélyes fenyegetést jelentenek Vietnamra?
- Mit tehet Vietnam a számítógépes fenyegetések enyhítésére?
- Hogyan tud Vietnam együttműködni a nemzetközi szervezetekkel e kockázatok megoldása érdekében?
- Milyen előnyei vannak a visegrádi stratégiáknak a más országokkal szembeni számítógépes támadások elleni védekezésben?
- Milyen kiberbiztonsági stratégiákat találtak Vietnám számára az alkalmazkodás szempontjából?

A kutatási hipotéziseket az alábbiakban mutatjuk be. Terjedelmi korlátok miatt az értekezés főként a visegrádi országok és néhány szomszédos vietnámi ázsia-régió kiberbiztonsági stratégiáira összpontosított, hogy javaslatok készüljenek új kiberbiztonsági keretre Vietnam és szomszédos országai számára.

2. Hipotézisek

1. hipotézis (H1): A visegrádi országokban a kiberbiztonság megosztja a hasonlóságokat a célok, a stratégiák és az erők között, hogy összehangolják az Európai Unió tagállamait a fegyveres erők, a kiberbiztonság és a nemzetbiztonság tekintetében.
2. hipotézis (H2): A kelet-ázsiai és a délkelet-ázsiai országok kiberbiztonsága egy biztonságosabb társadalom létrehozását és a gazdasági fejlődést támogatja.

2a. Hipotézis (H2a): Szingapúr kiberbiztonsági stratégiája adaptálható Vietnam jogi keretéhez.

3. hipotézis (H3): A virtuális biztonság, különösen a visegrádi országokban a kiberbiztonsági együttműködésben, az ázsiai országokkal, különösen Vietnamban és annak szomszédai részére adaptálható és hálózatba foglalható.

2. Kutatási módszertan

A tanulmányban összegyűjtött adatok tudományos cikkek, a visegrádi országok által használt kiberbiztonsági stratégiákkal kapcsolatos szakirodalmi áttekintés meta-elemzése az EU, az ENISA, a NATO, a CCDCOE és hasonlókkal. Ezenfelül a kiberbiztonsági szolgáltatók cégeivel több szemléletet vontak be a kiberbiztonsági szakértőkkel, hogy azonosítsák a számítógépes fenyegetéseket, a számítógépes bűncselekmények és a számítógépes támadások veszélyeit, valamint az azok ellenőrzésére szolgáló módszereket.

4. Eredmény

Az értekezés általánosságban áttekintette a számítógépes bűnözést (ember által előidézett támadások és gépi támadások) és annak típusainak nemzetbiztonsági aspektusait, azok negatív és eltérő hatásait a kormányzati szintű biztonságra és a polgárok életére; különösen a nemzet gazdaságában, pénzügyeiben és információs infrastruktúrájában. Ezen túlmenően ez az értekezés különösen megmutatta az ázsiai országok közötti kétoldalú és többoldalú együttműködéseket a biztonságban és a gazdaságban, valamint a kereskedelem, a katonai, az energia, a béke, a barátság és a diplomácia területén az ASEAN-országok számára. Ezen túlmenően a dolgozat legfontosabb szakmai hozzájárulása az, hogy jelentős különbségeket ad a kiberbiztonsági együttműködésben Ázsia és az EU között. A doktori értekezés tudományos hozzájárulása az, hogy világossá tette a kiberbiztonsági együttműködést a V4-országok között, amelyekben az EU egyik középpontjában a nemzeti stabilitás erősítése, a számítógépes fenyegetések csökkentése, a kapcsolat erősítése és a kiberbiztonság, a számítógépes biztonság javítása valamint az EU, a NATO és más szervezetek közötti védelem vagy más jövőbeli kihívások állnak. Ezen kívül ez a tanulmány áttekintést nyújt az ASEAN országok nemzetbiztonsági stratégiájáról és jelenlegi kihívásairól, a számítógépes incidensekről, a kiberbiztonsági együttműködés nem megfelelőségéből adódó gyengeségekről.

5. Lehatárolások

Először is, a kutatási adatok korlátozottak voltak, mert ez a téma egészen új volt. Továbbá a biztonsági információk egyes területei érzékeny információk; ezért az azokhoz történő hozzájutás is biztonsági korlátozási problémákat viselt magán, nagy részük nem nyilvános információ. Másodszor, az időkorlátok miatt csak korlátozott számú interjú készült kiberbiztonsági szakértőkkel, amik értékesebb útmutatást és információt adhattak.