Connecting Communities: the answer to cybersecurity challenges

Dr. Ferenc Suba

Vice-Chair,

European Network and Information Security Agency

Senior advisor,

Prime Minister's Office, Hungary

Main messages

- NATO/EU/Member States articulating the need for co-operation with non-military/non governmental actors
- Growth of national/governmental CERTs and ISACs
- CERTs are in the position to connect military/government and private sector at the operational level, ISACs at the decision making level
- Need for a common interface (strategic + operational levels)

NATO's co-operation with non-military actors

- concept of "in-depth cyberdefense," endorsed at the 2010 NATO summit in Lisbon

- civilian authorities in all member nations have the lead responsibility on cybersecurity.
- NATO in support of whole-of-government approaches to cyberdefense — led by civilian agencies in each nation — and with actors outside government.
- Key among non government actors: commercial suppliers + the wider industrial base (NATO-wide, 85 percent of critical infrastructure is in private hands)

NATO Cyber Defence Policy + EU Cybersecurity Strategy

NATO CDF:

- Develop minimum requirements for cyber defence of national networks critical to NATO's core tasks.
- Provide assistance to the Allies to achieve a minimum level of cyber defence and reduce vulnerabilities of national critical infrastructures.
- Engage with partners, international organisations, the private sector and academia (awareness-raising, sharing of best practices)

EU CST:

- 2.3. Developing cyberdefence policy and capabilities related to the framework of the Common Security and Defence Policy (CSDP)
- dialogue and coordination between civilian and military actors in the EU –exchange of good practices, information exchange and early warning, incident response, risk assessment, awareness raising and establishing cybersecurity as a priority

Evolution of CERTs in Hungary – from academia to state

- HunCERT: ISPs CERT operated by academia (1996)
- NIIF-CSIRT: CERT of the academic network (1998)
- CERT-Hungary I.: national and governemental CERT operated by Theodore Puskás Foundation (2004)
- govCERT-Hungary II.: national and governemental CERT operated by National Security Special Service (2013)
- CIP CERT: Ministry of the Interior, National Directorate General for Disaster Management (2013)
- MILCERT: Ministry of Defence (2013)

ISAC

US

- Started in 1998
- 16 sectors covered by 2014
- February 2015: presidential order on ISACs
- September 2015: first „model” ISAC by DHS

EU

- EU FI-ISAC in 2008 supported by ENISA
- Energy ISAC supported by EC in 2013

International best practice

- EU FI-ISAC, EU-SCIE, Meridian, IWWN
- Impetus: large incident, personal threat, simple envy
- Method: NDA, TLP (confidential but non-classified info!)
- Challenge: different communities/mentalities
  - CERTs: informal, effective, trust based
  - Banks, multinational companies: closed, business secret + interests
  - Governments: formal procedures, FOI, receiving mode
- Lifecycle: 3 steps
  - Big incident/push from above
  - Exercises (comcheck => complex)
  - Mutual learning (CERTs more formalised, Banks more open, Govts more flexible)
- Problems: NDA vs. FOI, trust vs structures, spying

Way ahead

NATO, EU, Member States:

- Connect private, government and military CERT communities + ISACs

CERT community:

- Trust based operation enhanced by formal procedures (e.g. international crisis management, data protection, transition of teams)

ISAC community:

- Cover all related critical sectors

All communities:

- Better understand and adjust to each other’s mentality (e.g. non-disclosure of shared information, informal relationships + formal procedures, common interfaces)