</V4 Cyber Security Infrastructure>

STRATPOL

Source: Asya Metodieva: Disinformation as a Cyber Threat in the V4: Capabilities and Reactions to Russian Campaigns, Stratpol 2018

Read: **bit.ly/cyberV4**

Czech Republic

/ key strategic documents

- National Cyber Security Strategy 2015-2020
- Action Plan for the NCSS 2015-2020

/ law

- Act No. 181/2014 Coll. (January 2015)

/main coordinating body

Under: National Security Authority (Czech Republic)
- National Cyber and Information Security Agency (NÚKIB)

/civilian cyber monitoring/capabilities

Under: Ministry of Interior
- Centre against Terrorism and Hybrid Threats (CTHH)

Under: Government of the Czech Republic; Parliament Committee
- Security Information Service (BIS)

/military cyber monitoring/capabilities

Under: Ministry of Defence
- Communications and Information Systems Agency (AKIS)

Under: Ministry of Defence, Military Intelligence (VZ)
- National Cyber Forces Centre (NCKO)

*Expected to be fully operational in 2020

/emergency response

Under: NÚKIB
- Government CERT (govCERT.cz)

/international cooperation

- NATO CCD COE (Tallinn) and STRATCOM COE (Riga)
- Hybrid COE (Helsinki)
- EEAS East STRATCOM Team (Brussels)
- NATO Cyber Coalition and Crisis Management Excersises

Slovakia

key strategic documents/

- Cyber Security Concept of the Slovak Republic 2015-2020
- Action Plan of Implementation of CSC SK 2015-2020

law/

- Act No. 69/2018 Coll. (January 2018)

main coordinating body/

Under: Parliament Committee
- National Security Authority (NBÚ)

civilian cyber/ monitoring/capabilities

- Ministry of Finance

Under: Government of Slovakia
- Slovak Information Service (SIS)

military cyber/ monitoring/capabilities

Under: Military intelligence (VS), Ministry of Defence
- Cyber Defence Centre (CKO)

*Based on new legislation entering into force April 2018

emergency response/

Under: National Security Authority (NBÚ)
- Computer Emergency Response Team (SK-CERT)

Under: Ministry of Finance
- Computer Security Incident Response Team (CSIRT.SK)

international cooperation/

- NATO CCD COE (Tallinn)

Hungary

/ key strategic documents

- National Cyber Security Strategy 2013

/ law

- Act L. on Electronic Information Security of Central and Local Government Agencies (2013)

/main coordinating body

Under: Ministry of Interior
- National Cyber Security Coordination Council

/civilian cyber monitoring/capabilities

- National Security Authority (NBF)

Under: Ministry of Interior
- Counter Terrorism Centre (TEK)

Under: Ministry of Interior, National Cyber Security Centre (since 2015)
- National Electronic Information Security Authority

Internal Intelligence
- Constitution Protection Office

External Intelligence
- Information Office

/military cyber monitoring/capabilities

- MilCIRC and MilCERT

/emergency response

- National Cyber Security Centre

Under: National Cyber Security Centre
- GovCERT-Hungary

/international cooperation

- NATO CCD COE (Tallinn)

Poland

key strategic documents/

- Cyber Security Strategy 2016-2020
- Cyberspace Protection Policy (2013)
- Cybersecurity Doctrine (2015)

law/

- Law on Cyber-Security (2018)

*Signed by President Duda in August 2018

coordinating bodies/

- Ministry of Defence
- Ministry of Digital Affairs

civilian cyber/ monitoring/capabilities

Internal Counterintelligence
- Internal Security Agency (ABW)

Under: Ministry of Interior
- STRATCOM Department

military cyber/ monitoring/capabilities

Under: Ministry of Defence
- Military Computer Incident Response Team (MIL-CERT PL)

Under: Ministry of Defence
- National Cryptology Centre

emergency response/

Under: Internal Security Agency (ABW)
- Computer Security Incident Response Team (CERT.GOV.pl)

international cooperation/

- NATO Counter Intelligence COE (Krakow)
- NATO CCD COE (Tallinn) and STRATCOM COE (Riga)
- Hybrid COE (Helsinki)

STRATPOL

INFOGRAPHIC BY: *ONDŘEJ ZACHA*

2018 · STRATPOL - Strategic Policy Institute · office@stratpol.sk · +421 908 893 424 · www.stratpol.sk