Red faces in Estonia over ID card security flaw | Financial Times

Estonia suffered an embarrassing blow to its much-vaunted ID cards that underpin everything from electronic voting to online banking, just days before hosting a big EU exercise on cyber warfare.

International scientists have informed Estonian officials that they have found a security risk that affects almost 750,000 ID cards and that would enable a hacker to steal a person's identity.

The Baltic country of just 1.3m people stressed there was no evidence of a hack of what it has proclaimed to be the world's most advanced IT card system. The cards are used to access a wide range of digital services from signing documents to submitting tax returns and checking medical records, as well as by foreigners who are e-residents in the country.

"The Estonian digital society is using cutting-edge innovative technologies. Those new technologies provide good value and services for the public, but may also impose risks," said Taimar Peterkop, head of the Estonian Information Security Authority.

Ministers say it will take several months to find a fix during which time the cards — issued since October 2014 — will stay in circulation. Electoral officials have yet to decide whether the cards can be used for electronic voting in next month's local elections.

The news comes as Estonia prepares to test defence ministers from across Europe on how they would combat a cyber war waged against them.

Armed with computer tablets at an informal summit in Tallinn on Thursday, the ministers will be faced with a series of scenarios that highlight how their Baltic hosts want to thrust digital security up the agenda of their EU presidency this year. Details of the two-hour exercise are being kept secret, but Estonian officials say it will have several dimensions including a simulation of an attack aimed at disabling military assets.

"It's purely fictional but we try to reflect the reality as much as possible," said Tanel Sepp, deputy head of the cyber policy department at Estonia's defence ministry. "Cyber has become a conventional tool in modern warfare."

Estonia is also keen to explore more widely whether EU rules in areas governing collective security and defence can be applied to the cyber realm. The European Commission is expected to review the EU's cyber security strategy by this month and to propose additional measures on cyber security standards, certification and labelling.

The exercise in Tallinn takes place amid a swirl of claims of political hacking and misinformation campaigns allegedly linked to Russia, which shares a border with Estonia. Toomas Hendrik Ilves, who was Estonia's president when the country came under the wide-ranging 2007 cyber attack, urged greater collective action this week on digital security at both EU and Nato levels.

Cyber has become a conventional tool in modern warfare

Russia has denied claims of being involved with political hacking.

Stung by the cyber attack a decade ago, which took down systems such as online banking, Estonia created a single agency responsible for cyber security and prioritised a “collective brain” approach of wide information-sharing about digital attacks and threats. It has created a separate cyber command in its armed forces, as well as a cyber-defence unit in its voluntary Defence League.

Adam Meyers, vice-president of intelligence at CrowdStrike, a US cyber security company, said wide co-operation had proved important in combating previous large-scale cyber attacks. He cited how security engineers, law enforcement officials and internet service providers had worked together in 2014 against the GameOver Zeus malware that US authorities say was used to steal millions of dollars by acquiring banking and other credentials.

“Organisations such as Nato and the EU can use their collective knowledge and capabilities to build a collective defence,” Mr Meyers said. “Even just knowing who to call during a cyber attack — you need to have a relationship with those people.”