Cyber defence

HOW TO TURN OPENNESS AND TRANSPARENCY TO A COUNTRY'S ADVANTAGE EVEN WHEN IT RELATES TO NATIONAL SECURITY?

Introduction

RESISTANCE

Estonia understands that the risk of cyber attacks will always be part of the information society — a risk that must be taken seriously. When Estonia was hit by a wave of cyber attacks in April 2007, we could focus on deflecting the attacks because we were thoroughly prepared and all parties knew how to behave. Estonia was hit by one of the largest coordinated cyber attacks against a single country. Regardless of the coordination and sheer volume of the attacks, they caused no major damage, and ultimately our response proved more important than the attacks themselves.

Narrative

OVERCOMING OBSTACLES

Estonia decided to make the attacks public unlike many cyber attacks that are kept hidden. The attacks were a wake up call for Estonia, indicating that in order to effectively prevent cyber threats, we must begin to prevent them on an international scale. One country is no longer enough. Following the attacks, Estonia gathered its entire strength to do something unprecedented — the establishment of an international coalition against cyber threats. As the ringleader, Estonia outlined the need to deal with cyber security, the value of practical experience and the work ahead, so that countries with similar democratic values could join the programme.

Estonia had had a unique experience and the successful deflection of the attacks made Estonia a credible voice. This changed the attitude of many countries toward cyber attacks and today cyber threats are considered part of modern warfare.

Results

EXAMPLES, FACTS

What is the outcome of an open and public attitude? Nearly a year after the attacks, the NATO Cooperative Cyber Defense Center of Excellence was established in Estonia to concentrate on applied research in the cyber field, including analysis, information sharing, training, and exercises. This is one of the most important organizations dedicated to cyber security in the world.

The handbook that focuses on the implementation of international humanitarian law in the case of electronic attacks is called "The Tallinn Manual".

The EU IT Agency, situated in Tallinn since 2012, is tasked with the development, protection and management of all EU-wide security IT-systems (SIS, VIS and the Eurodac information system for asylum seekers). Thanks to our open approach, the defence of the European Union's critical information systems and the NATO cyber security think tank are led from Estonia.

Conclusion

PUNCH LINE

More than sixteen years on, one of the most talented international cyber communities tackling highly sophisticated cyber security challenges is now concentrated in Estonia. Nobody could have imagined that the 2007 cyber attacks would have turned Estonia into a world leader in cyber security.

What doesn't kill you, makes you stronger. Estonia did not sheepishly wait for what would come next, but adopted the role of a daring test pilot and reacted differently to how cyber threats and attacks had been dealt with in the past, and found support from around the world.