Estonia after the 2007 Cyber Attacks:
Legal, Strategic and Organisational Changes in Cyber Security

Christian Czosseck, Cooperative Cyber Defence Centre of Excellence, Estonia

Rain Ottis, Cooperative Cyber Defence Centre of Excellence, Estonia

Anna-Maria Talihärm, Cooperative Cyber Defence Centre of Excellence, Estonia

ABSTRACT

At the time of the state-wide cyber attacks in 2007, Estonia was one of the most developed nations in Europe regarding the ubiquitous use of information and communication technology (ICT) in all aspects of society. Relaying on the Internet for conducting a range of business transactions is common practice. But naturally, the more a society depends on ICT, the more it becomes vulnerable to cyber attacks. Unlike other research on the Estonian incident, this paper does not focus on the analysis of the events themselves. Instead, the authors examine Estonia's cyber security policy and subsequent changes made in response to the cyber attacks. As such, the authors provide a comprehensive overview of the strategic, legal, and organisational changes based on lessons learned by Estonia after the 2007 cyber attacks. The analysis is based on a review of national security governing strategies, changes in the Estonia's legal framework, and organisations with direct impact on cyber security. The paper discusses six important lessons learned and manifested in actual changes: each followed by a set of cyber security policy recommendations appealing to national security analysts as well as nation states developing their own cyber security strategy.

Keywords: Cyber Attacks, Estonia, Legal Framework, Lessons Learned, Organisational Changes, Strategy

1. INTRODUCTION

Over three weeks in the spring of 2007, Estonia was hit by a series of politically motivated cyber attacks. Web defacements carrying political messages targeted websites of political parties, and governmental and commercial organisations suffered from different forms of denial of service or distributed denial of service (DDoS) attacks. Among the targets were Estonian governmental agencies and services, schools, banks, Internet Service Providers (ISPs), as well as media channels and private web sites (Evron, 2008; Tikk, Kaska, & Vihul, 2010).

Estonian government's decision to move a Soviet memorial of the World War II from its previous location in central Tallinn to a mili-

DOI: 10.4018/ijcwt.2011010103

tary cemetery triggered street riots in Estonia, violence against the Estonian Ambassador in Moscow, indirect economic sanctions by Russia, as well as a campaign of politically motivated cyber attacks against Estonian (Ottis, 2008). By April 28th the cyber attacks against Estonia were officially recognized as being more than just random criminal acts (Kash, 2008). The details of the weeks that followed are described in Tikk, Kaska, and Vihul (2010).

The methods used in this incident were not really new. However, considering Estonia's small size and high reliance on information systems, the attacks posed a significant threat. Estonia *did not* consider the event as an armed attack and thus refrained from requesting NATO's support under Art. 5 of the NATO Treaty; instead, the attacks were simply regarded as individual cyber crimes (Nazario, 2007; Tikk, Kaska, & Vihul, 2010) or "hackitivism" as established by a well-known information security analyst Dorothy Denning (Denning, 2001). A further discussion on whether or not the 2007 attacks were an armed attack is beyond the scope of this paper. Many defence and security analysts have covered this particular topic and discussed, e.g., the "juridical notion of information warfare" (Hyacinthe, 2009), a "taxonomies of lethal information technologies" (Hyacinthe & Fleurantin, 2007), formulated a "Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict" (Brown, 2006), or "legal limitations of information warfare" (Ellis, 2006).

The incident quickly drew worldwide attention, and media labelled the attacks the first "Cyber War" (Landler & Markoff, 2007). This led to an overall "cyber war hype" that was continuously carried forward by media, researchers and policymakers. This exaggerating rhetoric was employed during following conflicts like Georgia 2008 or Kyrgyzstan 2009, and such misuse of terminology has already received a fair amount of criticism (Farivar, 2009).

The 2007 attacks have shown that cyber attacks are not limited to single institutions, but can evolve to a level threatening national security. Looking back, the Estonian state was not seriously affected since to a larger extent state functions and objects of critical information infrastructure were not interrupted or disturbed (Odrats, 2007). However, nation states did receive a wake-up call on the new threats emerging from cyber space, alongside with new types of opponents.

The following three sections will provide a comprehensive overview of major changes in Estonia's national cyber security landscape, namely the changes of national policy. As a result, several laws and regulations were introduced, while others were amended, and there were several changes in the organisational landscape.

This paper features six lessons learned that were identified as most remarkable in the case study of Estonia. It concludes with several strategic cyber security recommendations.

2. DEVELOPMENT OF NATIONAL STRATEGIES

The benefits as well as threats of the use of Internet-related applications to information societies are identified by a number of Estonian high level policies and strategies.

The *Estonian Information Society Strategy 2013* (Estonian Ministry of Economic Affairs and Communication, 2006), in force since January 2007, promotes the broad use of ICT for the development of a knowledge-based society and economy. Given that cyber attacks on a scale matching that of Estonia in 2007 were unseen and likely unpredicted so far, it is not surprising that the risk of massive cyber attacks was not taken into serious consideration in the strategy – nor in other national policy documents from that era (e.g., the implementation plan of the Information Society Strategy for 2007-2008, Estonian Ministry of Economic Affairs and Communication, 2007)

The *National Security Concept* of Estonia published in 2004 (Estonian Ministry of Defence, 2004) and the government's action plan in force at this time (Estonian Government, 2007) were no exception since these documents did not even mention possible cyber threats or related actions.