Government of Cyber Security as National Security

MSocSc (Doctoral Candidate) Mirva Salminen

University of Lapland, Finland

msalmine(at)ulapland.fi

In the past years, cyber security has been defined as an aspect of national security in Finland. The reasoning has been related to the increasing complexity of the society, its overarching cyber-dependence and the indisputable intertwinedness of external and internal as well as physical and digital security. In order to safeguard functions vital to society in all security situations the government has commenced cyber security strategy and implementation process.

Finland's cyber security strategy and its background dossier were published in 2013, the implementation programme in 2014. In addition, as a member state of the European Union, Finland accommodates the union's cyber security strategy (2013) and its implementation. In the current stage of the implementation programme, all levels of state administration (central, regional and local) in all administrative branches are developing their cyber security planning, preparing, execution and evaluation. As a result, authority and responsibility are being reallocated within and between administrative branches. Coordination groups are assembled to direct the effort. Novel legislation and regulation are initiated and approved. Organisations are given new tasks or new organisations are being established. Cyber security speech has entered seminars, exercises and is gradually finding its way to office corridors. National cyber security emerges and is fitted to the pre-existing model of comprehensive security.

This article scrutinises the government of cyber security as national security. It examines practices – both discursive and material – through which national cyber security becomes and sustains its position as a 'real' societal factor that directs the conduct of people and organisations. Coexistent are practices through which information security is partially being replaced and hidden from sight or incorporated in cyber security. Discursive practices are patterns in the use of language that strategically direct the inter-subjective construction of cyber security as national security. Material practices are, for example, organisations and institutions such as rules, regulations and standards that co-participate in the aforementioned inter-subjective construction of cyber security. Together these material and discursive practices both reflect and constitute the structures in which national cyber security emerges. Moreover, they limit the pool of cyber security actors and mould these actors to be (in)compatible with one another.

The article asks how the objects and subjects of cyber security are being constituted in the Finnish national cyber security strategy and implementation process. Moreover, it examines relationships between and amongst these objects and subjects. Instead of trying to understand relationships as causes and effects that make national cyber security a complex system, it focuses on the government of conduct of people and organisations that are moulded to be cyber (in)secure. In other words, national cyber security is in the article understood as a complex, adaptive system, which simultaneously is a governing structure within the society. This structure consists of the relationships between and amongst objects and subjects of cyber security. These relationships are reflected in and constituted by both discursive and material cyber security practices. However, the strategic aim of these practices is not so much the flawless operating of technical systems and networks as the correct conduct of people and organisations. People are to behave in a preferred, cyber secure manner in their daily lives, which are already saturated by information and communication technology. They are to know what is right or wrong, smart or stupid and legal or illegal in the cyber-physical environment and submit to the authorities of national cyber security. Organisations are to ensure by the means of continuity management that their operations will not be

disrupted or halted due to digital interference. Cyber security is hence not understood as a technological stage, condition of the digital environment or a desired end-state but as a system for governing behaviour. It is an essentially social structure, which simultaneously reproduces the state as the main provider of security in society – even if in the role of supreme coordinator of the national cyber security effort – and allocates novel powers to other security providers.

Finally, the article scrutinises the effects which defining of cyber security as an aspect of national security has on national security in Finland. Reconfiguration of the role of the state was mentioned in the previous paragraph. In addition, relationships within and between administrative branches are reforming themselves – as are relationships between public and private actors. Multinational corporations are carrying out an increasing share of national cyber security work as national security is seen to cumulate from the level of the individual all the way to the level of international. The state cannot and is not willing to meddle with all these levels directly whereas corporations claim to be able to provide solutions for everyone. Corporations thus become important producers of national security – even if their role is merely mentioned in the Finnish national cyber security strategy. Simultaneously, more and more is required from individual citizens who are to know how to behave in the cyber-physical environment in a manner that minimizes the harm potential. At the other end of the spectrum, transnational cooperation is seen as a must because no society can produce its national cyber security without collaboration.

All the aforementioned developments are known. However, what new this article brings into the discussion is a careful analysis of the practices through which these developments take place.