ABSTRACT

The following dissertation studies the question how cyber security has become a national security agenda and discusses implications of the observed processes to current international security status quo. I divided the research into three parts. The first part embodies theoretical and methodological approach. The second part studies three distinct discourses related to cyber security, the techno-geek discourse, the crime-espionage discourse and the nation-defense discourse using the method of Michel Foucault about archaeology of knowledge. The third part then draws on these three discourses and discusses implications through lens of several theoretical perspectives. Namely through concepts taken from science and technology studies, from actor network theory and network assemblages. The critical point of the research is a distinct reading of these discourses. While techno-geeks are understood as a source of semiosis, hackers' capability and crypto-anarchy ideology influenced by cyberpunk subculture, the cyber-crime and espionage discourse is read as a source of evidence of the hackers' capability. The inspiration in popular subculture is combined with current efforts in development of liberating technologies against oppression by authorities, oppression recognized by the eyes of the crypto-anarchist movement seeking the world without state regulation or nation states completely. If these visions of near future inspired by cyberpunk are combined with the evidence of cyber crime, I argue, that we can observe an emergence of overemphasized imaginations on a national security level, the national cyber defense that gives birth of cyber as a national security agenda. In the discussion part, I am elaborating on different kind of expertise, the first driven by curiosity and the second driven by policy. Whereas the former would tend to understand the natural dynamics, the latter reacts on policy requirements based on beliefs. As both, natural and cultural sources, are influencing our perceptual field on the given problem, we can observe a proliferation of hybrids into cyberspace governability. Cyber security as a national security agenda has been able to develop its own church of knowledge that is covered by policy driven expertise reacting on the security imaginations; however, certain technical characteristics are surely making systems vulnerable. The inability to distinct between the cultural and the natural source is rising technological radical uncertainty, which subsequently fuels the imaginations of a needed national cyber defense. However, as states are raising their national cyber defenses they were being caught in a supermassive surveillance operation against their own citizens, which is certainly fueling the will of crypto-anarchist movement to develop more liberating technologies. More liberating technologies driven by actualized power of crypto-anarchists means lower immanent power to nation states. In the end, I argue that if nation states continue to strengthen their power and the construction of panopticon by arguing with needed defenses against imagined cyber terrorists and continue to lower privacy and freedom of citizens, we might be heading toward a world of hybridized governance, towards an emergence of oligopticon, in which states do not play the most significant role of a sovereign actor