Chapter 19
Russian Cyberwarfare Taxonomy and Cybersecurity Contradictions Between Russia and EU:
An Analysis of Management, Strategies, Standards, and Legal Aspects

Kimberly Lukin
University of Turku, Finland

ABSTRACT

This article analyzes the similarities and differences between the EU's and Russia's cyber preparedness, management structures, governmental security controls and cyber strategies. In comparing the cyber capabilities of the EU and Russia, we use military tactics and criteria as a basis for evaluating tactical, operational and strategic maturity. Russia has implemented cyberwar part of military strategic movements and certain taxonomy can be recognized in Russian based cyberattacks. Furthermore this study evaluates the following criteria: what are the EU's and Russia's procedures to prevent cyberwar, how their situational awareness is gathered and shared and is cyber used alongside with other military weaponry and tactics. This study claims that Russia has a better cyber war fighting capability than the EU countries. Based on the findings and recommendations in our article information can be used to create new threat models, to detect cyberattacks and finally point towards action to develop governmental cybersecurity in the EU.

INTRODUCTION

Since the collapse of Soviet Union, scientific and political communities have doubted Russia's war fighting capability, ability to form situational awareness and their capacity to conduct large scale warfare. However in its latest conflicts Russia has proved that cyber has maximized the power of strike when used

DOI: 10.4018/978-1-5225-7912-0.ch019

alongside the traditional war fighting methods. Even though the idea of common defence policy for the EU started in the end of the Cold War, issues such as forming a multinational preparedness level and the ability to lead military based cyber operations are not yet been implemented. Both EU and Russia have history of weakening their critical level preparedness. Russia had to re-create itself without its strategically important Soviet era military bases and telecommunication networks which were left to Eastern Europe after the independence of the post-Soviet states. Furthermore most EU countries preparedness level was systematically reduced after World War II.

The EU is an interesting benchmark for Russia since it has developed itself by becoming more like a state and is enhancing its defence capabilities. The EU via its institutions and bodies speaks on behalf of all its member states, representing and upholding the interests of the EU as a whole. Furthermore the EU provides an integral part of the legal system of its member states. By comparing EU and Russia we obtain important information on their abilities to use cyber as an extension of policy and how it is implemented as part of governmental management structures. Russia has no official military strategy at the moment except a nuclear strategy (Lieutenant colonel Forsström, P., personal communication, September 23, 2014), but cyberwar methods, new weaponry and Russia's recent conflicts are re-creating a strategic baseline. Even though political tension between the EU and Russia has risen in recent years, the EU has not proceeded with a creation of power structures for managing its member states cybersecurity. The actions taken have rather been legal frameworks and policies which limit its ability for intelligence based operations in telecommunication networks. The EU's sanctions against Russia based on the Ukraine conflict might escalate new conflicts in near future, which is why it is crucial to understand how capable the EU countries are of defending their values and sovereignty against cyberwar actions. Moreover, each EU member state is responsible for developing its own cyber strategies. This creates a major contrast to Russia which developed without any publicity its cyber capability; which weakens predictability. Russia's policy in conflicts is to react via the military when political consensus cannot be created. Russia has taken many necessary actions in political conflicts whether they were accepted or not by international norms and laws, which naturally gives them the opportunity to use all needed methods, such as cyberattacks.

Countries have not realized that they need to prepare for situations when a global political or economic occurrence, for example an energy crisis might cause political tensions between countries and encourage the use of cyberattacks targeted at paralyzing critical functions. Quite often a cyber strategy is taken as separate entity and it is not tied to other strategies, management structures or traditional war fighting methods. Although strategic goals are often defined, the operational methods and tactical level are missing. The Cyber Hub (Cyber Power Index, 2012) has ranked the 20 most powerful cyber countries, evaluating countries' abilities to recover from cyberattacks. Russia is in the 14th place because it did not succeed in legal and social-economic contexts, and surprisingly also not in technology infrastructure. The research, however, did not take into account governmental management structures which are very crucial in leading recovery actions and preparedness. Moreover, the survey did not take into consideration the fact that Russia already had an information security doctrine in 2000 which stressed the importance of information security and was as a pre-act in a cyberwarfare context. The renewed military doctrine which was published in 2010 emphasized for the first time the role of information security in modern warfare and the usage of new weaponry which might refer to cyberattacks. Both of these doctrines defined necessary actions to protect information space. Russia has conduct systematic analysis of the content and nature of modern wars which has fostered implementation of cyber methods to war fighting skills. The Russian Duma considers cyberwar an integral part of information warfare and therefore is it is impor-