Increasing Robustness in the Network Society: A Comprehensive Approach to Cyber Security in Sweden

Johan Sigholm
Department of Military Studies
Swedish National Defence College
Stockholm, Sweden
johan.sigholm@fhs.se

This paper discusses the emerging digital threats that our increasingly connected network society is faced with. It considers a strategy based on collaboration and information sharing between civilian and military agencies aimed at increasing societal robustness in a small, yet highly connected country with limited resources.

The term *Network Society*, first coined in the 1990s by Jan van Dijk (2006) and Manuel Castells (1996), refers to a societal structure formed by the abundant access to information and communication technologies (ICTs), allowing information to be generated, processed and distributed on the basis of the knowledge accumulated in the nodes of the network. In the network society, government decision making and public service delivery are conducted by increasing use of advanced ICTs (Yang and Bergrud, 2008). ICT is also leveraged to create new and improved public services, for more efficient service provisioning and for reduction of operating expenses.

However, as information becomes pervasive, complex intersystem dependencies are formed that may induce serious vulnerabilities. These vulnerabilities can manifest as single points of failure in critical infrastructures, but also as an increased exposure to antagonistic threats such as cyber attacks. Mitigating the vulnerability of our increasingly technology-dependant society has therefore become a high-priority task for many governments and administrations of technically mature countries with well-developed ICT infrastructures. In Sweden, commonly ranking among the top countries in the world when it comes to ICT use, cyber security has become an increasingly important issue.

In 2010, the Swedish government decided to develop a national strategy for the protection of critical public services and infrastructure. The work was initiated by the identification of sectors containing functionality that continuously needs to be upheld in order to guarantee delivery of basic societal services, such as power production, water and food distribution, voice and data communications, emergency health care and financial services. These highly important societal functions are faced with several threats; traditional ones such as natural disasters and large-scale accidents may lead to disruptions limiting the access to goods and services. There are also new threats, brought on by the transition to a network society.

Preparing for these extreme events is an obviously difficult task, not least since they are unexpected by nature and hard to characterize in detail. When it comes to cyber security, this holds even more true. Not only is the target hard to predict, but the method of attack and the extent of the resulting consequences are often difficult to fully evaluate. A challenging problem is the initial classification of a cyber attack – as a criminal act or a military aggression. Since the identity of the attacker is commonly unknown, and since information flowing through computer networks is oblivious to geographical boundaries, an attack emanating from a server physically located in a certain country could in reality be initiated by a person in the same country as the victim, or equally by a government-sanctioned entity in an unidentified hostile nation.

Creating a robust network society requires a systematic analysis of existing threats, which vulnerabilities they may exploit, what assets that are involved and an assessment of the resulting risk. Several countries have invested substantial resources in building new lines of defense against the emerging digital threats, where the U.S. is probably the one that has come the farthest by the establishment of its Cyber Command. Sweden is in these circumstances a quite small country, geographically the size of California but with a population not exceeding 10 million. Even though the degree of national ICT development is high, the available resources for dealing with the threat of large scale hostile cyber attacks are limited, both when it comes to civilian agencies and the armed forces. Combining resources in a comprehensive approach to cyber security is thus needed in order to achieve effect.

A focus on increased collaboration, information exchange, education and combined exercises between the stakeholders responsible for responding to cyber attacks is most likely a key factor in increasing robustness of the network society. Besides reactive resources, which can be used to mitigate the consequences of an attack, proactive methods and assets are also needed to prevent an attack from succeeding or to limit its consequences. Signals intelligence and information operations have proven to be useful methods in this work and an extensive cooperation between parties possessing these capabilities is thus highly valuable. One must also realize that technology itself will not solve any problems, either civilian or military, but the focus must instead be on how it is used and in what context.

References

Castells, M. (1996) *The rise of the network society*, Blackwell, Oxford, UK.

Van Dijk, J. (2006) *The Network Society*, Second edition, Sage, London, UK.

Yang, K. and Bergrud, E. (2008) "Civic Engagement in a Network Society: An introduction", in K. Yang & E. Bergrud (eds.) *Civic Engagement in a Network Society*, Information Age Publishing Inc., Charlotte, NC, USA.