Kimberly Lukin

Requirements for Finland's National Cyber Security Strategy

Turku Centre *for* Computer Science

TUCS Technical Report
No 1037, February 2012

Requirements for Finland's National Cyber Security Strategy

Kimberly Lukin
University of Turku, Department of Information Technology

TUCS Technical Report
No 1037, February 2012

Abstract

EU countries have prepared weakly against cyber war. Although cyber warfare is not a new topic only in recent years it has been taken as a part of national security strategies. Many countries have not understood the meaning of centralized IT security and cyber security leading model. This study will show how governmental IT security and cyber leading structures should be formed and what technical protection methods are needed in order to protect country against cyber attacks. If IT security and cyber situation awareness is not formed in and lead from one centralized Ministry or Office, and recovery actions are not practiced; this kind of a country is wounded during disturbance and exceptional situations. Instead of large scale investments at once military performance could be increased in a short term with researching the weaknesses of other countries national IT security and by creating attack vectors and practicing offensive cyber attack methods. At the same time it would be clever to start planning and investing in IT security of governmental and critical infrastructure organizations by creating frontline network and sensor to protect governmental and CIP organizations. The most expensive task would be creation of Ministry of Safety or office responsible of leading IT security and cyber preparedness. However, if it is done at first, it would slow down the development of military performance and it is unifying to other military domains, like air and ground forces.

Keywords: cyber security, critical infrastructure protection (CIP)

TUCS Laboratory
Communications Systems

1. Cyber war

War fighting methods are evolving but rarely new methods have lead into entire defense reform as cyber war has done. Cyber warfare refers operations made via computer networks, for example use of viruses and malicious programs either the intelligence purpose or hamper systems of target organizations or countries.

Alongside the traditional methods of warfare cyber war gives superiority through the destructions of the other party's information infrastructure or by causing break in the information flow to the operative intelligence systems. This means that moving the troops to the right position and obtaining and sharing information might become more difficult. Cyber attack might destroy industrial automation systems and nuclear power plant systems and at worst case cause nuclear exploitation or destroy electricity distribution network.

1.1. Background of Finnish national cyber security strategy

In Finland there is no cyber security strategy, units or specially educated staff to execute cyber war attacks, or methods and structures to recognize large scale attack types against critical infrastructure organizations. Finnish national IT Security Strategy will not give a uniform objectives and methods to raise the level of national IT security. Even Finnish defense Force has not yet cyber security strategy, Finnish Ministry of Defense established workgroup in 2011 in order to create national cyber security strategy which should be ready in the end of 2012 (YETT, 2011).

Finnish government should prioritize their unambiguous IT projects before cyber strategy is ready. Their synchronization problems and the abundant number of the projects might be reason that timetables have failed in IT Security Level (The Ministry of Finance, 2010) and ICT-preparedness projects (ICT-contingency, 2009) and costs have been higher than in original action plan estimated.

In Finland again several military garrisons have been abolished because of the increasing need of Defense Force savings. There is also need to invest in new cyber domain since it is new type of weaponry alongside with other domains: air, space, sea and ground forces. In the USA cyber will be 5th domain (Economist, 2010). In Finland four domains has its own commander. Time shows will cyber reach that important position in Finnish defense forces.

Cyber war has been formed of IT security and hacking, so it is a combination of passive and active methods. With IT security operational and critical infrastructure systems are protected but furthermore IT security will give backup for cyber warfare operations

enabling untraceable hacking and intelligence operations via networks. Furthermore in most cases without knowledge of IT security weaknesses of target systems, cyber attacks could not be executed and attack vectors could not be aimed properly. In cyber war new dimension is created when it is tied to part of the other traditional war fighting methods, like in the case when air force could use unmanned aerial vehicles (UAV) to conduct interference against target systems.

2. National cyber security strategy model

National cyber security strategy model should be based on cyber domain, which according to this study consists of six subsections. The most important section of cyber domain is the control structure of state IT safety because country can´t lead preparedness, form picture of situation awareness and lead recovery actions without it. Cyber strategy is an execution model, which defines concrete methods.

2.1. Cyber domain

According to this study cyber domain should consist of:

1. State structures give platform which support the preparing and the cyber operations. There should be one ministry which is knows the information security level of all the state institutions and critical infrastructure organizations and is capable to form situation awareness, analyze and share information and lead cyber operations.
2. National critical infrastructure. Big part of national critical infrastructure belongs to the hands of private sector. There is a need for cooperation between government and public organizations.
3. Protection of electronic equipments and electromagnetic spectrum related to data storing, modification and information exchange between networks. There is increasing need to study and test new protection methods like cryptographic protection and self learning and defending networks
4. Management systems in which it is possible to combine and analyze real time information
5. Active defense, which includes forefront network and sensor, which will use pattern recognition to detect viruses and other network threats, vulnerabilities and attack vectors.
6. Practice of offensive cyber methods and influencing methods. There is a need to find methods to affect against attackers systems, sensors, information and ability to do interception and interference.

2.2. Legislation

Finnish legislation will not allow the usage of cyber attacks against other countries as part of national protection. Hence, the national legislation is not familiar at all with the concept of cyber security, particularly if country has a need to use cyber attacks as a method in the conflict. The legislation should be examined for both national and international legislation. This requires both the developing of the national judicial know-how and international cooperation.

However, just protecting governmental and critical infrastructure organizations against cyber attacks is not sufficient method. In Finland public administration and the private sector should be involved in the security planning and part of risk analysis so that their position and task in cyber security is obligated with contracts. Either, Finnish legislation has not been prepared for the grey stage which is the final level before actual war. In a situation like this the extended cyber attack can affect dangerously to the vital functions of the country. Critical Infrastructure organizations (like air line and maritime companies and telecommunication operator) should be bind with the legislation and contracts so they would be under the command of Finnish government. This bond might affect to the economic losses but above all it could cause wider reactions such as internal revolts when the citizens would not be able to utilize telecommunication networks like phone calls and internet. In the agreements, attention must be paid to the sufficient amount of the staff to the maintenance of vital functions. This matter should be taken to process during the new term of office. The law would clarify operation if new Ministry of Security or Office could be established in Finland.

With the methods of the legislation should restricted outsourcing of the vital functions and the maintenance of high classification level operative systems. The legislation should be examined for both national and international legislation. This requires both the developing of the national judicial know-how and international cooperation.

2.3. Leading structures

In Finland IT security leading has been decentralized between different ministries which has prevented the creation of uniform objectives in IT security. This has led to the situation that all the branches of administration have developed its IT security and IT functions independently for decades without centralized control.

In Finland there is also lack of the strategic leading, because control of centralized coordination of governmental IT functions and the overlapping of the IT projects and workgroups cause difficulties to achieve common objectives. In Finland IT security is lead by three ministries: national IT security belongs to the Ministry of Finance, international IT security cooperation to the Ministry for Foreign Affairs and national IT strategy for the Ministry of Communications. Finland is the only country in European

Union where Ministry of Finance leads n IT security. This causes the fact that the IT security and cyber preparedness control is not in independent hands. The competition of funds and power between the ministries causes internal fragmentation and the lack of the management.

According to cyber security strategy of Germany the responsibilities of cyber security leading has been decentralized (Cyber Security Strategy for Germany, 2011). However, if the IT security and cyber security is not directed from one centralized Ministry, there is not centrally formed situation awareness and recovery actions are difficult to practice and this kind of a country is wounded during disturbance and exceptional situations. In the other states of Europe, governmental IT security is not lead by the Ministry of Finance since their responsibility is financing and the economic follow-up of IT projects but not controlling them.

It is crucial how IT security control responsibilities are lead in governmental level and how responsibilities are divided, because in recovery situations there must be one organization that has IT security situation awareness, know the security level of all governmental and critical infrastructure organizations, and is able to lead recovery processes. Also Competition (funding and leadership issues) between Ministries may jeopardize national IT security and international cooperation and visibility to foreign countries, comprehensive responsibility of IT security looks like Finland is not well organized in security leading. The reorganizing of the public administration would require the shutdown of old functions as it was done in Great Britain. In Finland creation of the Safety Ministry or office has to be considered.

2.4. Needed changes

It is remarkable how Russia succeeds after collapse of Soviet Union raise its combat capability and cyber war capability only within 10 years, for which I refer to Russia's possible inclusion to cyber attacks in Estonia's Bronze soldier case (The Guardian, 2007) and during Russia's war to Georgia (CCOCOE, 2008) just a few to mention. Russia has been claimed orchestrating cyber attacks to steal national secrets (Independent, 2011). Interesting point is that Russian government has never actually been caught up but instead Russia's hacker groups has taken the reputation of attacks. Russia has used cyber war techniques more commonly and effectively than western countries and therefore raised its combat ability quickly. Even Russia is not as strong as it was in a days of Soviet Union, it have learned to focus its power to new forms of warfare. Cold war has given us a lesson that the amount of weaponry might not be important. Modern warfare requires that there are well protected, encrypted and fast network management system between important cities and countries, ability to analyse information and find weak points of enemies IT systems and infrastructure.

1. There is a need for the ministry which directs both IT security and cyber security of state institutions, has situation awareness and is also capable to lead cyber security operations and recovery situations.
2. Cooperation between the public sector and the country is needed because large part of National critical infrastructure is in the hands of private sector.
3. National cyber strategy and budget is needed. Government must identify what cyber space is and its significance as a new warfare method.
4. Cyber security strategy has to be executable and it should raise war fighting ability in a short term. It should include enforcement program and it should be feasible and carried out at certain time and on certain budget. It should have sub programs like research (in order to create vulnerability library of the weaknesses of the other countries IT systems), practicing of offensive cyber methods, protecting governmental and critical infrastructure organizations and creating defensive IT network and sensors, establishing of safety ministry or unit which can lead both IT security and cyber security. Strategy itself need to be shared to executable action plans in otherwise it might slow down like happened in UK because there was no metrics, time plan and independent audit. (Computerworld, 2012).
5. Finland needs the law of telecommunication network interception
6. The establishment of cyber security unit and groups. Cyber security unit what should be own domain
7. Finnish government should increase the own amount of the technical expertise. State organizations which has role in preparedness should secure their own amount of technical expertise, especially in the case of confidential IT system
8. It would be important to link national cyber security strategy into other national strategies like The Security Strategy for Society (Finnish Ministry of Defense, 2010) and National Information Security Strategy (OECD, 2003) so that they would support each other's and would emphasizes their mean in national security. Finnish government should estimate how the common EU strategies and threat estimates of the union are reflected to Finnish strategies. Attention has not been paid to these.
9. International cooperation and information exchange, to conclude the agreement on the common objectives and information exchange. Cooperation should be information exchange between countries about cyber attacks. Russia and China have suggested that Internet should be under government control and censored, but UK has issued it would be fatal and human rights should concern Internet too (Guardian, 2011)
10. Clarification of national NCSA´s role so it could maintain functions properly. Nowadays it's organization which is not able to fulfill all its obligations which have been given to it. The preparing fails out without the efficient multinational cooperation.

11. Implementation of the Security Strategy for Society's (YETT) should include concrete action plans prevention of new threats like cyber war. It should be linked to all other security strategies in Finland. Since preparing requires resources which on small countries are not often found Finland needs cooperation's with other countries. Common situation awareness with the EU single intelligence analyzing capability SIAC cooperation could be solution.
12. CSIRT needs authority position (power to take action). Preparedness will fail without effective international cooperation. Finnish government should estimate how strategies and threat assessment of EU will effect to Finnish national security strategies like the Security Strategy for Society (Finnish Defense Ministry, 2010) and The Security Strategy for Society (YETT). Also should estimate what is Finland's role in a part of EU security society. Lisboan summit should be used to form cyber security partnership between EU countries.
13. Government should support long term cyber security research. Finland needs long-range and systematic study of the field of cyber security which would support the development of Finnish technical innovations which increase the ability of the country to prepare for endangering threats. The study of the long term safety must also be supported with the research institutions and with the private sector. The developing of the technology must be continued and must be tested with the research institutions and with the private sector. Finland should technical safety solutions of other countries. Long-range and systematic study of the field and company work, both supporting the development of Finnish technical innovations which increase the ability of the country to prepare for endangering threats. The developing of the technology must be continued and must be tested with the research institutions and with the private sector The study of the long term safety must also be supported with the research institutions and with the private sector, cyber.
14. Government should support the developing of new innovations.
15. The active protective measures are needed and it should be possible to prevent the threats at an early stage. It improves the ability of the country to track and to defend against cyber war.
16. It is not sufficient that only Finnish defense forces networks are defended, also companies which belong to national critical infrastructure protection plan (CIP) need to be defended. It should be solved how does the society change information and operates together in the exceptional situations? Protection instructions and actions need to be done regarding also CIP organizations
17. Clarification of the role of governmental roles and instructions to the companies is remarkable that meaning of technical demand is clear and executable. Otherwise it distorts the competition of small companies who wants to have contract with government.

18. Government must identify that cyber security and cyber war has significance as a new base of warfare method. It need relevant budget and cyber security should be lead by one organizations.
19. Government should have ability and right to track attacks and take needed actions.
20. Increase country's ability to track and to defend against the threats improving the delivery of cyber products and services, to industry and increasing investment, in national intelligence capabilities. In Finland there is not enough technical IT security product development and innovations like in Russia where government support development of encryption products.
21. Government should practice people to identify, protect and inform against IT security threats
22. Cyber warfare should be part the traditional war fighting methods of the warfare and have its own cyber strategy and budget
23. Cooperation with other countries especially the ones which are cyber security forerunners
24. Draw up the methodology of the protection in administrative and operative networks during grey stage
25. The international cooperation and preparing improve Finland's ability to anticipate the development of the threat of the safety and demands to the protection. the developing of the safety requires an international information exchange inside, for example in EU. Cyber security development should be tied for the national safety, Finland should do an agreement on the common objectives, and from information exchange in Scandinavian level with Sweden and Norway.
26. Lisbon Summit was signed in 2009 in EU which means mutual assistance of countries during crisis, but not yet in cyber security level. There should be agreement for the information exchange before and during possible crisis. Finland should also examine, own, national, safety and the defense political strategies partly the strategies of the EU and deal common objectives proactively in the branch of IT security and cyber war in order to prevent cyber war.
27. Finnish government should decide if they want to be part of EU´s own cyber security program or create own of northern defence ally which would be good since EU and Sweden has "cleanest networks in the world". It could be "virtual defense ally"

2.5. Technical counter acts

According this study in cyber security and war main focus is in technical protection methods, surveillance and attack methods.

1. Cyber war methods could be teach for people in military service if attack methods, analyzes of network attack vectors and sensors are made via user interface tools like consol and software which will hide attack structure and methods, like usage of botnets. Since actual hacking methods take time to learn and skills need to be maintained regularly this could be solution. There also should be hired cyber units which launch more sophisticated attacks.

2. Attacks against embedded systems are increasing. Since they control larger system like the engine in an airplane, weapons systems, networked sensor and industrial systems they are major cyber attack targets in the future. There should be self protection mode which isolate part of system or put it into another "manual" mode when it is not working as it was designed to, it should have "inner authentication" methods which continuously recognize deviations. Security should be part of architectural design, processes, implementation, protocols and cryptographic algorithms which should protect system against abuse.

3. Application and crypto security play major role. Governmental institutions and CIP organizations should have a baseline (software development standard or NCSA´s recommendation of reliable crypto software for government concerning high security level information systems.

4. Basics of cyber defense are technical IT security actions like: encryption methods, beaconing detection, surveillance, patch management, vulnerability scanning, Intrusion Prevention, but also higher level surveillance which includes sensors, pattern recognition which can recognize attack vectors should be also implemented.

5. Surveillance methods like national GovCert/Csirt processes need to be defined.

6. Technical actions for protecting operational networks and electromagnetic spectrum are needed.

7. There is a need for management system where situation awareness and distributed information from CIP organizations, ministries, military domains, intelligence and other organizations and information sources is shared and analyzed to the use of ministries

8. Active defense which needs cyber units and technical surveillance equipments

9. Practice of cyber war- There is need to find methods with government can effect to attackers information systems, sensors, information and ability to do interception and interference.

10. Government should concentrate to the application security (protects its embedded systems, operational systems), decide and give standard or framework whether to use open source or COTS applications and list of recommended and standardized techniques to public administration. Inspection of foreign applications of the field of

information security and cryptography should draw the line what methods are safe to use in CIP and governmental organizations.

11. Ensure that in Finland and to other countries network and telecommunication connections between most important cities are ensured, encrypted and exceptional situations have been practiced that they connections work in every situations (weather conditions, interception, and interference)

12. Governmental operative systems, application security standards, architecture (divide between operative and governance network) and platform of systems should differ from non-classified systems. There is a need for "front line network" which prevents attacks to the critical infrastructure.

13. Interception of communications would give possibility to create automated monitoring and tracking methods in order to prevent cyber terrorism. Because in Finland privacy issues are in high level, interception law should be prepared concerning just automated surveillance methods. Since attackers in cyberspace have ability to be initiative and take the advantage interception of communications is most important preventive act if it is combined with cyber security actions.

14. Attacks against cryptographic systems are increasing. Governments should pay attention to quality of static cryptographic methods and usage of dynamic crypto methods.

15. Viruses, malwares and Trojans are cyber warfare tools which should be used for intelligence and destruction. Country should have own laboratory to produce new generation of computer viruses.

16. In Finland there should be technical level conversations in expert level regularly. Technical expert pools could produce useful information for the use of governments since in most cases decision makers are not technical persons and they also don´t have wider understanding of their own work or governmental area.

2.6. Action plan

In the military level defensive and offensive cyber security capability could be raised within 3 years. During the first year national and international contacts and cooperation model should be created. Establishing cyber unit and reorganizing government might take a longer time because of the political issues, in a mean time attack methods could be practiced in laboratory conditions. In the base of cyber attack practices military should have vulnerability library about weaknesses of other countries IT systems and

practice offensive and protective methods. While governmental organizations robust their IT systems military should create defensive network together with governmental organizations and private sector. It would take first wave of attacks, protect critical infrastructure since its censors would measure the network traffic. Remarkable enough cyber domain also needs its own budget, security branch and commander to be independent from other ministries and to be a credible military branch.

2.7. Conclusion

Cyber security domain is often characterized hard to define. According to this study cyber domain will define methods to protect critical infrastructure, practice to launch cyber attacks and the leading structures. For government it will take years to build a new domain of warfare. Governmental cyber domain has three levels. First level will define governmental structures that are needed to lead cyber preparedness and cyber war actions (The ministry or office which will lead governmental and critical infrastructure organizations IT security and cyber preparedness). Second level defines how to protect critical infrastructure and governmental information systems and surveillance systems. Third level defines what cyber war is, it investigate offensive methods, network based intelligence and creates vulnerability and attack vector library against different countries. Furthermore it defines how cyber war methods could be used as part with other war fighting methods (like HPM, satellite destruction).

On the base of cyber strategy there should be knowledge what is the actual state of Finnish governmental IT security, adequateness of technical protection level and the weak points in the systems of Ministries and Offices are. Information like that will help to form cyber security action plans (sub programs which will ensure that strategy is feasible).

Cyber strategy will be successful if it has concrete action plans and programs with accurate mission, time table, funding and people and tracking points. Cyber strategy should tell cyber domain (IT security and cyber preparedness leading structures) and include concrete action plans like establishing cyber units, practicing cyber actions and technical protection methods.

Russia has succeed in usage of offensive cyber attack methods where EU counties haven´t. One reason is that Russia has working governmental command and control structures but they also have invested in cyber war methods and used them successfully in Georgia war (CCDCOE, 2008). EU countries have used great amounts of money to cyber security and have been forced to drive down some military functions in order to create new cyber units. Russia is a good example that they did not invest in large amounts of money for the cyber, but they still have capability to do cyber war successfully because they have developed offensive methods.

EU countries should be aware that cyber security defense capability should be raised level by level and described part of national cyber strategy. Preparing against new threats require resources which small countries usually do not have. Instead of large scale investments at once, at first it would be clever to increase the military performance in a short term with researching weaknesses of countries national IT security and creating attack vectors and practicing offensive cyber attack methods. Research of modern defence and war fighting methods are needed in order to prevent enemy superiority. The meaning of cyber strategy, units and utilizing them with other war fighting methods becomes from the fact that without them government cannot protect itself against the new threats.

Second task needed is to invest in IT security of governmental and critical infrastructure organizations by creating frontline network and sensor to protect governmental and CIP organizations. Technical projects, which will not improve and produce battle resistant results in a short term, are not advantage to the public administration.

Third and the most expensive task would be preparing and creation of centralized IT security and cyber security leading Unit or ministry. Hence, if it's done at first, it would slow down the development of military performance in the field of cyber security and it's unifying to other military domains, like air and ground forces. In Finland the coordination of all governmental IT security projects from one centralized place is missing so question is how government will lead cyber security action plans and cyber preparedness and rise cyber war fighting ability. This wakes the question would it be better establish Safety Office or Ministry which would direct all governmental IT security actions from one centralized place. That would give independent position without need to fight about funding or authority position. It's important not only establish organization which lead cyber security and preparedness but also lead governmental and critical infrastructure organizations IT security because security situation awareness is needed on the background of cyber security and warfare. The most critical thing is that cyber domain needs its own budget, commander and it should be considered as new domain (defense branch) to be independent war fighting method.

In the military level cyber capability could be raised fast if offensive and defensive cyber attack methods are practiced (in laboratory conditions) and vulnerability library of other countries IT systems are created. While governmental organizations robust their IT systems military should create with the help of government and critical infrastructure organizations frontline network and sensor in order to protect critical its infrastructure.. These actions could be done within three years.

References

[1] The Economist, War in the fifth domain, July 1st 2010. www.economist.com/node/1647892. Verified 2012-02-25.

[2] CCOCOE, Cyber Attacks Against Georgia: Legal Lessons Identified. Eneken Tikk, Kadri Kaska, Kristel Runnimeri, Mari Kert, Anna-Maria Talihärm, Liis Vihul. www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf. Verified 2012-02-25.

[3] Finnish Ministry of Defence, 16.12.2010, www.defmin.fi/?!=en&s545

[4] Computerworld, 10th January 2012, UK´s cyber strategy implementation ´too slow´ says former security minister. www.computerworld.co.nz/news.nsf/security/uk-cyber-strategy-implementaton-too-slow-says.former-security-minister. Verified 2012-02-25.

[5] The Guardian, Russia accused of unleashing cyberwar to disable Estonia, 17th May 2007, www.guardian.co.uk/world/2007/may/17/topstories3.russia. Verified 2012-02-25.

[6] The Guardian, FBI and Homeland security launch probe as foreign cyber attackers target U.S water supply, 1th November 2011.Governments must not censor internet, says William Hague. www.guardian.co.uk/technology/2011/nov/01/governments-must-not-censor-internet. Verified 2012-02-25.

[7] Independent, 1th November 2011, China and Russia accused of orchestrating cyber attacks, www.indipendent.co.uk/news/world/asia/china-and-russia-accused-of-orchestrating-cyber-attacks-6255411.html. Verified 2012-02-25.

[8] ICT contingency, 19th March, 2009, www.vm.fi/cm/fi/04_julkaisut_ja_asiakirjat/20090318CTvara/11_ICT-varautuminen_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20090318CTvara/11_ICT-varautuminen_yhteenveto_19_3_2009.pdf. Verified 2012-02-25.

[9] The Ministry of Finance, 28th 2010. Instruction of IT security in Finnish government, VAHTI 2/2010. www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus_20101028Ohjeti/name.jsp. Verified 2012-02-25.

[10] OECD, 4th September, 2003. Finnish National Information Security Strategy www.oecd.org/dataoecd/38/0/36406236.pdf. Verified 2012-02-25.

[11] Cyber Security Strategy for Germany, 25th 2011, www.enisa.europa.eu(media/news-items/german-cyber-security-strategy-2011-1

[12] YETT, 2011, Security Strategy for Society, http://www.yett.fi/en/materials. Verified 2012-02-25

[13] YETT, Kansallinen kyberturvallisuusstrategiatyö on aloitettu, http://www.yett.fi/fi/ajankohtaista/90-kansallinen-kyberturvallisuusstrategiatyoe-on-aloitettu.Verified 2012-02-25

Turku
Centre *for*
Computer
Science

Joukahaisenkatu 3-5 B, 20520 Turku, Finland | www.tucs.fi

University of Turku
- Department of Information Technology
- Department of Mathematics

Åbo Akademi University
- Department of Information Technologies

Turku School of Economics
- Institute of Information Systems Sciences

ISBN 978-952-12-2717-2
ISSN 1239-1891