

Report to the Storting (white paper)

No. 38

(2016–2017)

Report to the Storting (white paper)

Cyber Security

A joint responsibility

1	SUMMARY	7
2	BACKGROUND, FRAMEWORKS AND THE CONTENTS OF THE REPORT	8
3	TRENDS AND THE IMPORTANCE OF CYBER SECURITY	9
4	CYBER SECURITY AND PRIVACY	10
5	A JOINT RESPONSIBILITY	13
5.1	PUBLIC-PRIVATE COOPERATION.....	14
5.2	INTERNATIONAL COOPERATION	14
5.3	CIVIL-MILITARY COOPERATION	16
6	PREVENTIVE CYBER SECURITY – BUSINESSES’ OWN ABILITIES.....	16
6.1	LEGAL REGULATION IN THE AREA OF CYBER SECURITY	17
6.2	ORGANISATION OF CROSS-SECTORAL RESPONSIBILITY	18
6.3	SYSTEMATIZATION AND DEVELOPMENT OF RECOMMENDATIONS AND REQUIREMENTS	18
6.4	OUTSOURCING	20
6.5	INTRUSION TESTS	21
6.6	KNOWLEDGE BASE	22
6.7	CULTURE AND LEADERSHIP	22
6.8	PRIVACY AND PREVENTIVE CYBER SECURITY	23
7	DETECTING AND MANAGING CYBER ATTACKS	23
7.1	THE WARNING SYSTEM FOR DIGITAL INFRASTRUCTURE	24
7.2	FRAMEWORK FOR CYBER INCIDENT MANAGEMENT.....	25
7.3	INFORMATION SHARING	26
7.4	DIGITAL BORDER DEFENCE	27
7.5	CYBERCRIME	28
7.6	COORDINATION BETWEEN NSM, THE INTELLIGENCE SERVICE, PST AND THE POLICE.....	29
7.7	OPENNESS ABOUT CYBER ATTACKS.....	30
7.8	ANALYSIS CAPACITY	30
8	CYBER SECURITY COMPETENCE.....	30
8.1	NATIONAL STRATEGY FOR CYBER SECURITY COMPETENCE	31
8.2	PRIMARY, LOWER AND UPPER SECONDARY SCHOOL EDUCATION	32
8.3	HIGHER EDUCATION	32
8.4	RESEARCH	33
8.5	POST-QUALIFYING AND FURTHER EDUCATION	34
8.6	COMPETENCE IN SUPERVISORY INSTITUTIONS.....	34
8.7	EXERCISES	35
9	CRITICAL ICT INFRASTRUCTURE.....	36
9.1	ALTERNATIVE CORE INFRASTRUCTURE AND ROBUSTNESS IN THE REGIONAL TRANSPORT NETWORKS.....	37
9.2	INTERNATIONAL CONNECTIONS	38
9.3	EMERGENCY AND PREPAREDNESS COMMUNICATION	38
9.4	CYBER SECURITY IN MANAGEMENT AND CONTROL SYSTEMS	39
9.5	PRIVACY AND CRITICAL ICT INFRASTRUCTURE – COMMUNICATIONS PROTECTION	40
10	ELECTRONIC COMMUNICATION	42
10.1	REDUCE THE CRITICALITY OF TELENOR’S CORE INFRASTRUCTURE	42

10.2	ENSURE DIVERSITY AMONG THE SUPPLIERS OF THE INFRASTRUCTURE	42
10.3	CREATE A CSIRT IN THE ELECTRONIC COMMUNICATION SECTOR DIRECTED BY NKOM	43
10.4	ACTIVE AUTHORITY BY THE MINISTRY OF TRANSPORT AND COMMUNICATION AND THE NATIONAL COMMUNICATIONS AUTHORITY	44
10.5	ESTABLISH MEASURES TO REGULATE THE HANDING OVER OF TRAFFIC DATA TO THE POLICE	45
11	SATELLITE-BASED SERVICES	47
11.1	CLARIFY A REGULATORY RESPONSIBILITY FOR NORWEGIAN SPACE ACTIVITIES	47
12	ENERGY SUPPLIES	48
12.1	STRENGTHEN SUPERVISION AND GUIDANCE IN CYBER SECURITY	48
12.2	STIMULATE GREATER AND SPECIALIST COMMUNITY WITH MORE RESOURCES WITHIN CYBER SECURITY	49
12.3	BUILD A STRONG OPERATIONAL SPECIALIST COMMUNITY FOR ICT INCIDENT MANAGEMENT	50
12.4	ASSESS SECURITY ISSUES BY THE PROCESSING AND STORING SENSITIVE ENERGY INFORMATION ABROAD	50
12.5	CONDUCT RISK AND VULNERABILITY ANALYSES FOR EXTENDED USE OF AMS	51
12.6	PREPARE AN UPDATED ANALYSIS OF THE POWER SUPPLY'S DEPENDENCE ON ELECTRONIC COMMUNICATION	52
13	OIL AND GAS	52
13.1	TRANSFER THE SECURITY TRADITION IN HSE TO THE DIGITAL AREA	52
13.2	ASSESS THE VALUE OF THE SECTOR'S FACILITIES AND ICT SYSTEMS AND ESTABLISH REGULATIONS FOR DIGITAL VULNERABILITIES	53
13.3	CLARIFY THE ROLE AND CAPACITY OF THE PETROLEUM SAFETY AUTHORITY	54
13.4	ASSESS THE CONNECTION TO THE RESPONSE ENVIRONMENT FOR ICT INCIDENTS.	54
14	WATER SUPPLY	56
14.1	INCREASE CYBER SECURITY COMPETENCE IN NORWEGIAN WATERWORKS	56
14.2	STRENGTHEN SUPERVISION AND GUIDANCE IN CYBER SECURITY	57
14.3	IMPROVED SYSTEMS FOR INCIDENT MANAGEMENT	58
14.4	CONDUCT RISK AND VULNERABILITY ANALYSES BEFORE POSSIBLE INTRODUCTION OF SMART WATER METERS	58
15	FINANCIAL SERVICES	59
15.1	STRENGTHEN EFFORTS TO ASSESS FUTURE PAYMENT SERVICES	59
15.2	CONTINUE INTER-DISCIPLINARY COOPERATION FOR GOOD PREPAREDNESS AND MANAGEMENT OF SERIOUS INTENTIONAL ICT INCIDENTS	60
15.3	ANALYSE THE VULNERABILITY CONSEQUENCES AS A RESULT OF OUTSOURCING OUT OF THE COUNTRY	61
15.4	CONTINUE AND STRENGTHEN COMMITMENT TO INFLUENCING INTERNATIONAL REGULATIONS OF CYBER SECURITY MECHANISMS	62
15.5	STRENGTHEN EMERGENCY MEASURES FOR THE DEVELOPMENT TOWARDS THE CASHLESS COMMUNITY	62
16	HEALTH AND CARE SERVICES	63
16.1	STRONGER MANAGEMENT OF CYBER SECURITY BY THE MINISTRY OF HEALTH AND CARE SERVICES	63
16.2	MORE RESEARCH ON CYBER SECURITY WITHIN NEW HEALTH AND WELFARE TECHNOLOGY	64
16.3	ESTABLISH SOLUTIONS TO MEET THE DEVELOPMENT WITHIN HEALTH AND WELFARE TECHNOLOGY	65
16.4	CONDUCT MORE ICT EXERCISES WHERE CRITICAL SYSTEMS ARE DOWN	65
17	TRANSPORT	66
17.1	STRENGTHEN ICT SUPERVISION AND COOPERATION BETWEEN THE TRANSPORT BRANCHES	66
17.2	ESTABLISH A JOINT REPORTING CHANNEL FOR ICT INCIDENTS WITHIN THE TRANSPORT SECTOR	67
17.3	SPECIAL MEASURES FOR SEA TRANSPORT	68
18	COMPETENCE	70
18.1	ESTABLISH A GENERAL NATIONAL SKILLS STRATEGY WITHIN CYBER SECURITY	70

19	CRISIS MANAGEMENT	70
19.1	INCREASED CYBER SECURITY COMPETENCE AT LOCAL AND REGIONAL LEVEL.....	70
19.2	STRENGTHEN EMERGENCY PREPAREDNESS AT REGIONAL AND LOCAL LEVEL.....	71
19.3	ESTABLISH A COMMON CLASSIFIED ICT INFRASTRUCTURE	72
19.4	ASSESS MEANS OF COMMUNICATION WITH THE PUBLIC.....	72
20	CYBER ATTACKS	73
20.1	ESTABLISH AND PRACTISE A COMPREHENSIVE FRAMEWORK FOR CYBER INCIDENT MANAGEMENT	73
20.2	IMPROVE THE NATIONAL OPERATIONAL CAPABILITY THROUGH CO-LOCATION (MAJORITY AND MINORITY)	74
20.3	INCREASE DETECTION CAPABILITIES AND COMPILE A SITUATIONAL PICTURE	75
20.4	STRENGTHEN CAPACITY AND EXPERTISE RELATED TO MANAGEMENT OF CYBER ATTACKS.....	76
20.5	ESTABLISH A NATIONAL CYBER CRIME CENTRE	77
20.6	ENSURE STRONG SPECIALIST CYBERCRIME UNITS IN THE POLICE DISTRICTS	77
20.7	ENSURE AN ICT INFRASTRUCTURE TO SUPPORT POLICE CRIME PREVENTION.....	78
20.8	ENSURE THE BALANCE BETWEEN PRIVACY AND A MORE SECURE SOCIETY.....	79
21	COMMON COMPONENTS	80
21.1	MONITOR THE DEVELOPMENT OF ICT OUTSOURCING OF COMMON COMPONENTS	80
21.2	DEVELOP COMMON PROTECTION MEASURES AGAINST SOPHISTICATED CYBER ATTACKERS.....	80
21.3	REGULATE ELECTRONIC IDENTITY	81
22	CROSS-SECTORAL INITIATIVES.....	82
22.1	ESTABLISH A NATIONAL FRAMEWORK TO ENSURE A COMPREHENSIVE ASSESSMENT OF VALUE CHAINS	82
22.2	CLARIFY REQUIREMENTS FOR BUSINESS MANAGEMENT SYSTEMS.....	83
22.3	CONSCIOUS USE OF STANDARDS	84
22.4	CLARIFY THE MINISTRY OF JUSTICE AND PUBLIC SECURITY'S ROLE AND AREA OF RESPONSIBILITY	85
22.5	STRENGTHEN THE MINISTRY OF JUSTICE AND PUBLIC SECURITY'S POLICY INSTRUMENTS	86
22.6	INCREASE CYBER SECURITY CAPACITY IN THE MINISTRY OF JUSTICE AND PUBLIC SECURITY	88
22.7	ADAPT THE SUPERVISORY ACTIVITIES TO INCLUDE CYBER SECURITY.....	88
22.8	AN ACCOUNT OF CYBER SECURITY SHOULD BE INCLUDED IN ANNUAL REPORTS.....	89
22.9	INDUSTRIAL AND COMMERCIAL DEVELOPMENT AND CYBER SECURITY	90
22.10	OUTSOURCING AND CLOUD SERVICES	90
22.11	REGULATION OF CRYPTOGRAPHY	92
23	FINANCIAL AND ADMINISTRATIVE CONSEQUENCES	94

Report to the Storting (white paper)

No. 38

(2016–2017)

Report to the Storting (white paper)

Cyber Security

A joint responsibility

*Recommendation by the Ministry of Justice and Public Security of 9 June 2017,
approved in the Council of State on the same date. (The Solberg Government)*