center for cyber- and information security

a shared commitment to the nation's research and expertise development

A perfect time for cyber crime

Norway's Telenor hit by cyber espionage campaign

Cyberbullying suicide

Cyber criminals run riot in India

Cyber war in Ukraine

Cyber attacks up 32% in 2013

U.S. Criticized For Cyberespionage Program

Hackers in China Attacked The Times for

Norway Cyber Attack Targets Country's Oil, Gas Systems

CYBER-ATTACK ON NORWEGIAN MILITARY

ID Theft Exposed 200M Consumer Records

Hack Attack

DDoS cyber attacks get bigger, smarter, more damaging

Under cyber attack

Cyber crime levels continue to rise

Nursing Homes Are Exposed to Hacker

Majority of organizations unable to effectively respond to cyber-attacks

Cyberattacks becoming a plague upon healthcare organizations

Increase in Cyber Attacks

Stressing Internet Costing Millions,

Cyberbullying 'on rise'

Girls Charged For Cyber-Bullying Girl Who Committed Suicide

Netbanking frauds top cyber crime charts

Business understanding of cyber attacks a decade out of date

NSA monitored calls of 35 world leaders after US official handed over contacts

Dark web 'will evolve', warns UK cyber crime chief Andy Archibald

Cyber, Economic Crime Is Growing

Brazil, Europe plan undersea cable to skirt U.S. spying

«Ungplug Big Brother»

Hackers Cost U.S. Economy Up To 500,000 Jobs Each Year, Study Finds

Hackers Cost U.S. Economy Up To 500,000 Jobs Each Year, Study Finds

The NSA Actually Intercepted Packages to Put Backdoors in Electronics

FBI Seeks Romanian Cyber Theft Ring

Cyber attacks on companies double

Hackers demand $300 'ransom' to halt huge cyber attack

Deutsch Centre Cyber crime levels continue to rise

Russia and Ukraine in cyber 'stand-off'

Cyber crime is threat to all

New study says Cyber bullying increases rates in suicides

eopolitical Tensions Invade Cyberspace

Posted at 05:27 PM ET, 06/01/2011

Google: Hundreds of Gmail accounts hacked, including some senior U.S. government officials

Telstra breaches privacy of thousands of customers

Norton says Cyber Crime Costs Mexico $3B Per Year

Telstra breaches privacy of thousands of customers

No, Your Small Business Is Not Safe From Cyber Attacks

India lost $8bn to cyber crime

Kickstarter Hacked

Hackers demand $300 'ransom'

Cyber attack shuts down local utilities computer

Are there enough cyber warriors to fight against crime?

Girls Charged For Cyber-Bullying Girl Who Committed Suicide

Dette systemet styrer produksjonsroboten til et Statoil-selskap

Ble varslet om minimal beskyttelse allerede i juli, men ingenting ble gjort.

Turns out young people want to be actors, not cyber security professionals

Cyber search engine Shodan exposes industrial control systems to new risks

Miss Teen USA Says Someone Hacked Her Bedroom Computer Webcam

Iranian cyber warfare commander shot dead in suspected assassination

Snowden files || Report suggests Israel behind attempt to hack into French communication network

UK cyber criminal behind £750,000 bank phishing scam jailed for five years

Cyber raiders hold Queensland firms to $3000 ransom by locking computer files

Massive Russian Cyber-criminal Campaign Targets Companies in India

NSA monitored calls of 35 world leaders after US official handed over contacts

'Cyber Jihad'

10 Reasons to Fear a 'Cyber Pearl Harbor'

Cyber-espionage: The greatest transfer of wealth in history

2

Nursing Homes Are Exposed to Hacker Attacks

Hacker targets South Houston sewer system

Majority of organizations unable to effectively respond to cyber-attacks

Computer Virus Brings Down Train Signals

Energy firm cyber-defence is 'too weak', insurers say

North Korea may have secretly engineered computer games to launch mass cyber attack

Business understanding of cyber attacks a decade out of date

Crypto locker virus holds computer and files ransom; demands $300-$700 (Video)

Cyber-Gang Targets Sensitive Industries With Flexible Botnet

Police warning after drug traffickers' cyber-attack

UK energy infrastructure 'at risk of shutdown from cyber-attacks'

UK becomes first state to admit to offensive cyber attack capability

North Korean 'cyberwarfare' said to have cost South Korea £500m

The Cyber-War Against Iran Is a Real War, and a Rehearsal for Future Conflicts

OUR INCREASED VULNERABILITY

Our increased reliance on Information and Communication Technologies (ICT) will create in the years ahead new, large, and increasingly complex security challenges; confronting these challenges will require an increased focus on higher education, more efficiency in resource development, improved research capacity, and broad cross-sector collaboration among industry, infrastructure providers, the police and other government security agencies, and academia.

In the last few years we have seen a number of examples of how everything from pacemakers and cars to electricity generators, public transportation, or intellectual property may be exposed to criminal activity and destroyed from a distance -even from the other side of the globe. Thousands of events have brought up information security and cyber security to the public debate, including security breaches in government computer systems, lack of protection of personal information, loss of credit card information, and espionage at high level. The virus that put 35,000 computers out of work in Saudi Aramco, the world's largest oil company; the cyber attack on Georgia, ahead of Russia's invading the country; industrial espionage against the Scandinavian telecom operator Telenor; the Americans' access to communication information in other countries; the cyber attacks on the Nobel Institute and the International Monetary Fund (IMF), the nuclear enriching programmes of Iran and Estonia; a strong increase in identity theft and relentless attacks on our financial institutions; and the Swedish monitoring law (FRA) that provides the Swedish intelligence service full access to the content of communications of their neighbour countries that is transmitted across Swedish soil.

It is said that what can go wrong will go wrong. ICT has opened up a whole new dimension of how things can go wrong -be it by themselves or due to malicious acts. We must be prepared.

6 EXAMPLES FROM AROUND THE WORLD

1 While 20,000 Norwegians are exposed to pickpocketing every year, 60,000 are victim of identity thefts that result in financial loss.

2 In March 2013 the telecom operator Telenor announced that several of its senior management team had been subjected to extensive and organised cyber espionage.

3 In the U.S. a cyber attack happens every three minutes on average. In December 2012, more than 55,000 computers at Saudi Aramco, the world's largest oil company, were incapacitated by a virus attack. 450,000 names and passwords were stolen from Yahoo in May 2012.

4 After *The New York Times* investigated allegations of economic nepotism among the Chinese prime minister's family members, the newspaper's servers and a number of laptops were tapped over several months. *The Washington Post, The Wall Street Journal* and several other newspapers and news media have experienced similar espionage.

5 Denial of Service attacks can be purchased online. The websites of the Nobel Committee were attacked when it awarded the Peace Price to a Chinese dissident in 2010, and later a number of organizations in Norway, including Norwegian security agencies, political parties, and businesses, experienced similar attacks.

6 Iran's nuclear program was delayed due to a targeted attack using the Stuxnet computer worm. When Norway joined military operations in Libya in 2011, the Norwegian Armed Forces were victim of a sophisticated attack.

"... an inadequate national focus on areas such as cyber security poses potential real threats to Norway's security."

"We must confront new dangers, like cyber attacks, that threaten our nation's infrastructure, businesses and people," President Barack Obama wrote in his introduction message to the 2014 budget.

Our new, large and increasingly complex security challenges require efficiency in the development of resources, training and research, sophisticated and dynamically evolving study programmes and applied research, and well developed relations among stakeholders and good collaboration across sectors.

However, the dramatic increase in cyber security challenges has demanded a focus on achieving operational capacity, creating a critical undercapacity in research and education. The funding for developing relevant skills and carrying out research is still limited, and collaborative relations between stakeholders and academia are poorly developed. All this is putting security stakeholders under pressure.

Some countries have responded to these challenges. For instance, the U.S. state budget for 2014 allocates $500 million to the Department of Homeland Security for cyber security research.

In the Nordic countries the response has been slower. For instance, an independent international committee evaluating ICT research in Norway concluded that Norway's inadequate national research strategy on cyber security "poses potential real threats to security in Norway." To this concern, the Center for Cyber and Information Security (CCIS) is an answer.

In Norway, the key national cyber security stakeholders have initiated a partnership to establish the Center for Cyber- and Information Security (CCIS), a national centre for research, training, and education in cyber- and information security.

Statkraft
Statkraft is Norway's largest energy production company and Europe's largest provider of renewable energy, it has clear cyber security responsibilities for the energy sector. Statkraft works actively on cyber security in various business areas, including hydropower, wind power, gas power, and distance heating.

Statnett
Statnett is responsible for Norway's national electricity grid, an infrastructure that is increasingly becoming dependent on ICT for its operations. Statnett is constantly working to develop a long-term cyber security strategy to strengthen its ability to deal with cyber security threats.

Eidsiva
Eidsiva Energy is a regional power producer and supplier and it is the largest in the eastern part of Norway. As a regional player, Eidsiva has undertaken a particularly supportive role for developing competence in the Innland region. CCIS' objectives and role are in line with Eidsiva's efforts to strengthen its own security strategy.

National Security Authority (NSM)
NSM is Norway's national security agency responsible for national cyber security, it operates the national Computer Emergency Response Team (NorCERT). NSM does threat analysis at national level working with experts on cyber security and cryptology.

Cyber Defence (CYFOR)
The Norwegian Cyber Defence is the branch of the Norwegian Armed Forces responsible for counter-cyber warfare in Norway.

Department for the Protection of Critical Infrastructure (BKI)
BKI is a division of the Norwegian Cyber Defence with duties that include the Computer Network Defence for the Defence Information Infrastructure of the Norwegian military. This involves the detection of computer network attacks and intelligence threats against ICT infrastructure, and the analysis and comparison of indicators of network attacks.

Norwegian Defence Research Establishment (FFI)
FFI is a multidisciplinary institute responsible for conducting research and development in order to

Center for Cyber and Information Security will become one of the largest academic environments in cyber- and information security in Europa and will position itself as a national resource and the contact point for international partners.

meet the targeted needs of the Armed Forces and for developing expertise in various aspects of defence.

Ministry of Justice and Public Security (JD)
The Ministry of Justice and Public Security is responsible for societal security and preparedness, crime prevention and correctional services, immigration, courts and the legislative work for law enforcement.

National Police Directorate (POD)
The National Police Directorate is responsible for Norway's police districts and special police agencies, with the exception of the Police Security Service (PST). PDO has undertaken responsibility for establishing closer contact between the police and the applied research sector in Norway.

Police ICT Service
The Police ICT Service was spun off from the Police Data and Material Services (PDMT) in the fall of 2013 and is responsible for developing and facilitating the police ICT infrastructure and applications.

National Criminal Investigation Service (Kripos)
Kripos is a special agency within the Norwegian Police Service with responsibility for investigating organized crime and major crime. It is Norway's contact point for Interpol and Europol and their respective competence centres for fighting cyber crime.

National Authority for Investigation and Prosecution of Economic and Environmental Crime (ØKOKRIM)
Økokrim is Norway's central unit for fighting economic and environmental crime.
Financial crimes of importance today are in one way or another perpetrated using computer equipment and often directed against computer systems. Challenges of economic crime include fraud related to identity theft and the identification and investigation of digital evidence and pattern tracking within large amounts of data.

Police Security Service (PST)
PST is the police agency for home security in Norway. PST will contribute its insight and expertise to CCIS in order to increase national security, enhance the ability to ward off, understand and investigate incidents, and

provide the Norwegian government with the best possible threat assessment and advice.

Oslo Police District
The Police at the Oslo Police District have established a strong unit in computer crime and international crime.

The Norwegian ID Centre (NID)
NID has a national responsibility for identity and document expertise. NID is a key partner with the Norwegian Biometrics Laboratory at CCIS.

Telenor
Telenor is a multinational telecommunications company headquartered in Norway, and one of the world's largest mobile telecommunications companies. Telenor owns major networks in 12 countries and has operations in 29 countries through its 33% ownership in VimpelCom. Telenor contributes into CCIS with its expertise in cyber security of electronic communications.

Mnemonic
Mnemonic is one of the largest specialists in information security in Norway, It delivers products and services to Norway's largest businesses, both in the public and private sectors. The company works strategically with long-term skills development goals in its own business and in its customers' businesses.

NC–Spectrum
NC-Spectrum delivers consultancy services in engineering, project development, and operation of infrastructure in the public and private sectors. NC-Spectrum works closely with its customers to develop cyber security for communication networks and critical infrastructure.

PriceWaterhouse Coopers (PwC)
PricewaterhouseCoopers is a multinational professional services firm. It provides a range of integrated cyber security services.

The International Business Machines Corporation (IBM)
IBM is an American multinational technology and consulting corporation. The company has several centres of expertise in cyber security.

Oppland County (OFK)
The Oppland County Council has been an early supporter of CCIS, a financing agent and a strong and enthusiastic promoter of CCIS. The County Council cooperates actively in the effort to improve information security in the county's municipalities and businesses.

The Norwegian Police University College (PHS)

The Norwegian Police University College is a public university college that offers education to the police force of Norway, including a three-year bachelor program in police studies. PHS conducts research in relevant areas including law, police science, criminology, psychology and sociology. PHS expands and develops its offer of study and its research programme to be at the head of understanding how to combat modern crime. PHS takes a central role in CCIS and helps the centre with a strong development of its expertise, research capacity and study programmes in various aspects of cyber crime.

Gjøvik University College (GUC)

GUC established its first research group in information security 11 years ago and has built it up to become one of Europe's largest open academic research groups in the field. Today GUC leads the National Research School in Information Security (COINS) and is offering dedicated undergraduate programmes in information security at bachelor, master and PhD level, in addition to its undergraduate programs at these three levels in Computer Science. GUC is currently Norway's most research-intensive college, and last year it fetched more research funding from the EU than almost all other university colleges in Norway combined.

Norwegian Defence Cyber Adademy (FIH)

FIH's study program awards bachelor degrees in military education to "cyber soldiers" and it develops research capacity in cyber defence. FIH cooperates closely with GUC.

Norwegian Centre for Information Security (NorSIS)

NorSIS has a national mandate to increase the information security expertise of individuals and businesses through raising awareness about threats and vulnerabilities, disseminating specific measures through the news, providing advice and guidance, and trying to influence positive attitudes in information security. NorSIS participation in CCIS will enhance the centre's ability to deliver a broad dissemination of knowledge and practices on information security and to this purpose it will collaborate with the local authorities and SMEs.

United for a Security Center

Gjøvik University College will establish a centre for information security with up to 80 employees and ten professors, with the participation of Defence, the National Police, Industry and Academia.

Leif Martin Kirknes - Computerworld, 11.06.2013

The initiative for the establishment of the Center was jointly presented at a press conference on 11 June 2013 by Major General Roar Sundseth, Head of Cyber Defence, Kjetil Nilsen, Director of National Security Authority, Odd-Reidar Humlegård, Director of the Police Directorate, Benedicte Bjørnland, Director of the Police Security Service, and Morten Irgens, Vice-Rector for Research at Gjøvik University College.

They described the centre and explained that the national program will be targeted and helpful, with a focus on collaboration, applied research and problem solving.

Official opening of the Center
August 15, 2014

The Center for Cyber- and Information Security

will strengthen our expertise and skills to prevent, detect, respond to, and investigate undesirable and criminal computer based activities.

The centre will undertake actions towards:

- Building research capacity and research groups at top level internationally in disciplines that are relevant for our partners and for Norway.
- Providing training and study programs of high quality and with great societal relevance.
- Contributing to Norway's international collaboration where partners can participate and apply their knowledge and expertise.
- Helping to increase the recruitment of students and researchers for the Norwegian education and training in security and for research environments.
- Contributing to the long term competence development strategy and research and education strategy.
- Cooperating with and contributing to organizations whose mission is to inform and raise awareness about security.
- Strengthening cooperation, exchanging knowledge, and sharing of skills among sectors, among application/innovation environments, among academic institutions, and among national and international projects, centres and organizations.
- Becoming a knowledge and expertise node in Europe's ability to compete for international research funding.

The 22 July Committee presents its report to the media

BROAD POLITICAL SUPPORT

CCIS has received strong interdisciplinary political support, including the direct and explicit support of several parliamentary committees and parliament's documents. The White Paper 207 S, (2011-2012), from the Special Committee report to the Minister of Justice and Minister of Defence from the Parliament's meeting held on 10 November 2011, concerning the attacks 22 July, explicitly and unanimously recommends that the Centre receives support. (Chapter15, page15): "The Committee welcomes the establishment of the centre and believes that the government should assess how the centre can be supported to develop its work".

"The White Paper 29 (2011-2012) on societal security has a separate section on the centre's initiative and describes a comprehensive task force that has been set up to consider further actions (Chapter 9, page 107). The Justice Committee decided to emphasise this in its report. Recommendation of the Justice Committee on terror preparedness (NOU 2012:14 Follow up Report of 22 July Commission) emphasises the importance of establishing Norwegian expertise in information security: "Especially the work carried out at GUC is of interest", points out the Committee in White Paper 207 S.

The Government supports the centre with 5 million NOK in 2014, from the Ministry of Justice and Public Security and the Ministry of Local Governments and Modernisation.

5 REASONS WHY THE CENTER IS IMPORTANT

1 The centre is important because an increasin amount of criminal activities are dependent on information and communication technologies (ICT). Crime, whether it takes place in cyberspace alone or not, most likely leave digital traces. At the same time it is a challenge to find, understand, assemble and secure such evidence in a way that it safeguard individual rights and forensic correctness.

2 The centre is important because the threat landscape changes. The increased mobility and open borders, climate change, increased unemployment and social pressures in Europe, resource scarcity, terrorism, pandemics and resistant infections, and Norway's participation in international military operations all help to increase the possibility of criminal acts, attacks and terrorism against Norwegians, Norwegian infrastructure and interests.

3 The centre is important because education, skills and research in cyber- and information security will help to combat increasing threats, vulnerabilities and offence in the cyberspace.

4 The centre is important because there is a need for extensive international cooperation and long-term research to prepare for tomorrow's challenges.

5 The centre is important because there is a need to educate and train new experts and to develop skills within the Norwegian central institutions, at the bachelor, master and PhD levels.

Every aspect of the challenge

Cyber- and Information Security is a discipline that must be understood in its full dimension, technological, psychological, social, economic, and organizational aspects interact and influence the outcome. Therefore, the centre promotes an exchange of knowledge and competence not only among academia and the applications areas, sectors, agencies and Institutions, but also among the different fields in cyber- and information security. Thus, CCIS academic degrees at bachelor, master and PhD level are specifically dedicated to information and cyber security. This is in contrast with how informations ecurity is taught most other universities, as some courses in a computer science degree.

The Center for Cyber- and Information Security (CCIS) is not only a research centre. It establishes competence transfer across agencies, companies and sectors. It facilitates research projects that connects industry and government agencies with international research networks. It connects research with study programmes and students to research, linking operational environments to academic study programmes and research. CCIS connects research, applications and study programmes with communication and dissemination capabilities.

center for cyber- and information security

CCIS delivers, through its core partners, a number of Bachelor programs in information security, network management and computer science, as well as a BSc in Telematics at the Norwegian Defence Cyber Academy (FIH), also known as the education of the military's "cyber warriors".

CCIS also delivers a MSc program in information security with three study tracks, information security management, forensics, and security technologies. The centre is also delivering a flexible, experience-based master with a a study track in the investigation of digital evidence and cyber crime, a collaboration between the CCIS paetners the Police University College (PHS) and GUC.

CCIS' dedicated information security programs cover the full scope of cyber and information security. In addition, the centre has a number of associated computer science programs at all levels with security-oriented activities, including security
applications of image and video processing, games and mobile computing technologies.

The Centre's PhD program in cyber- and information security will have 15 PhD students at start up in 2014 and 25 students two years later. In addition, the centre will have a number of associated PhD students in computer security research.

The centre provides flexible courses, training packages, corporate courses, and lectures. collaboration with the Norwegian Centre for Information Security (NorSIS).

PhD in Information Security

PhD in Computer Science

Master in Information Security

Master in Cyber Crime Investigation

Master in Applied Computer Science

Bachelor in Network Management

Bachelor in Information Security

Bachelor in Telematics

Bachelor in Software Development

Bachelor in Computer Engineering

One year program in Information Security

One year program in Software Development

Courses & training packages

Conferences, workshops, seminars

12 Study programmes

7 Study programmes dedicated to information security, cyber security, cyber defence and cybercrime, with:

20 PhD students

80 Master students

240 Bachelor students

Center for Cyber- and Information Security

Gjøvik University College

Police University College

Norwegian Defence Cyber Academy

NorSIS

center for cyber- and information security

Academic Network

Core research partners in CCIS includes Gjøvik University College, the Police University College, the Norwegian Defence Cyber Academy, and the Norwegian Defence Research Establishment. CCIS is developing substantial collaboration between these, on research, degree programmes, research network development, and international training programs. Each academic partner has quite different international networks, giving a strog potential for innovative international collaborations and research projects..

CCIS leads the Norwegian Research School of Computer and Information Security (COINS). COINS integrates Norwegian research groups in Information Security to a larger entity by integrating the course portfolio for research school members, builds stronger relationships between doctoral students in the network, establishes more incentives to excel and increases student mobility through access to a larger network. COINS also increases Norway's international student mobility, hosts internationally recognised researchers, and offers "free flow of goods and services" in Information Security Research in Norway. At any time, 40 PhD students are members of COINS.

COINS provides a significant added value to PhD students at CCIS, while CCIS provides COINS with a strong national and international network, including businesses, end users, and security agencies.

Norwegian University of Science and Technology - NTNU

University of Agder

University of Stavanger

University of Tromsø

University of Bergen

University of Oslo

Gjøvik University College

Police University College

Norwegian Defence Cyber Academy

COINS:
National Research School of Computer and Information Security

CCIS:
Center for Cyber- and Information Security

center for cyber- and information security

Focus Laboratories and Research Groups

The centre covers all major areas of information and cyber security. Multidisciplinary expertise is assembled in research groups and labs to address specific application areas.

Testimon Forensics Research Group

Mot crime today leaves digital evidence. The Testimon group develops new insight into digital evidence, computational forensics and various aspects of cyber crime. The group draws its core members from NISlab and the Electronics group at Gjøvik University College (GUC), the Police University College (PHS), the National Criminal Investigation Unti (Kripos), the National Economic Crime Unit (Økokrim), the ICT Crime Unit at the Oslo Police Department. and the National Securitya Authorities (NSM) The research group operates the forensics track of GUC's MSc in Information Security and the computer crime track of the experience-based MSc which is a collaboration between PHS and GUC.

The Norwegian Biometrics Laboratory

The Lab's research in physiological and behavioral biometrics includes 2D- and 3D-face recognition, fingerprint recognition , fingervein recognition, dental biometrics, ear recognition, signature recognition, gait recognition, keystroke recognition, gesture recognition and mouse dynamics. The lab also develops privacy enhancing technologies such as biometric template protection and integration in physical and logical access control. The lab has extensive biometric databases iand s an independent testing institution for biometric performance evaluations. The Biometrics lab is an active member in the European Association for Biometrics and co-organizer of the international conference BIOSIG as well as the Biometric Session of IEEE IIH-MSP. Its core members come from GUC and from the National ID Centre. The laboratory has partner organisations in nine different countries.

The Information Security Management Group

In a deeply digitized connected world, cyber- and information security threats cannot be seen from a technical point of view only. The Information Security Management Group develops cyber security models from socio-technical positions, which include social, legal, cultural, financial, political, and ethical aspects of security. The group has a special responsibility for the informations ecurity mangement track at the MSc in Information Security.

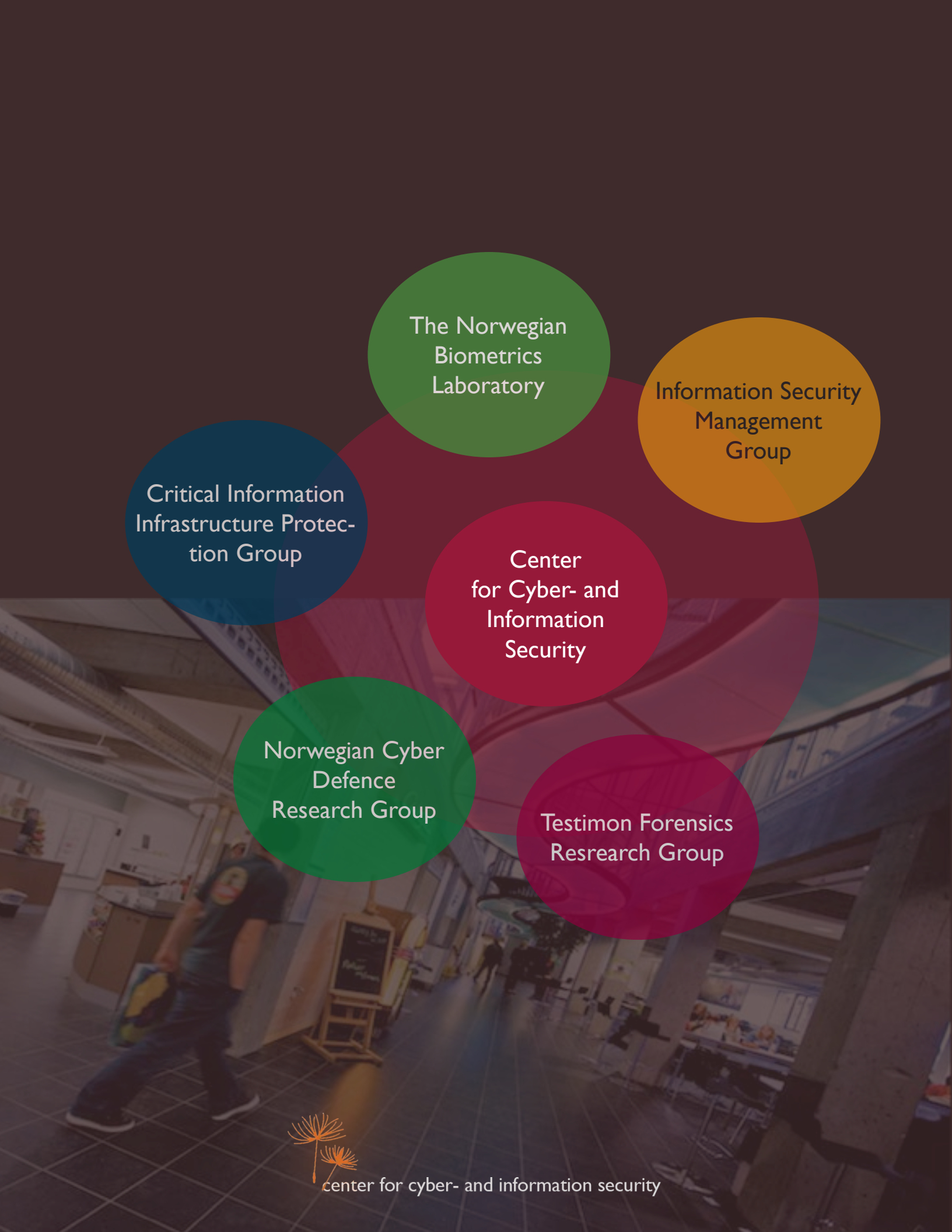
Critical Information Infrastructure Protection Group

The group is concerned with long-term research into the cyber security of industrial control systems / SCADA systems, distribution systems, monitoring systems, and real-time protocols. The group is also concerned with cyber security of the Internet of Things, which also includes cyber security of internet connected consumer objects. The core members come from GUC, Statkraft, Statnett, the National Security Authority (NSM) and Eidsiva.

Norwegian Cyber Defence Research Group

The research group specializes in various aspects of national cyber. It draws its members from the Norwegian Cyber Defence, GUC, the Norwegian Defence Research Establishment (FFI) and the Norwegian Defence Cyber Academy (FIH). The group contributes to the BSc, MSc and PhD programs in information security at GUC and FIH's BSc in telematics, known as the "cyber warrior" education.

Other research groups will be established, including information security in the health sector, product and software security and cyber security Innovation.



center for cyber- and information security

Associated Groups and Institutions

The Media Technology Laboratory (MTL)

CCIS shares offices with the Media Technology Lab. MTL delivers research and study programs (on BSc, MSc and PhD level) in various areas of computer science. Of particular interest to CCIS is its research in mobile security, biometric methods, user design for security and safety applications of augmented reality, mobile phones, tablets, game consoles, digital interfaces and visors (e.g. Google glasses). MTL's Colour and Vision Research Laboratory works in security with applications such as video analysis of gait recognition and the design of counterfeit-resistant bank notes.

NorSIS

CCIS will share offices with the Norwegian Centre for Information Security (NorSIS). NorSIS is part of the Norwegian Government's overall commitment to information security and reports to the Ministry of Justice and Public Security. NorSIS works to ensure that information security becomes a natural part of every day's life of citizens and businesses through raising awareness about threats and vulnerabilities and informing on security measures, NorSIS operates the online service *slettmeg.no* and the national identity theft project. With NorSIS, CCIS gets a partner highly experienced in communication, with an excellent network of SMEs, Norwegian municipalities and governmental agencies. NorSIS and CCIS will collaborate on media management, marketing resources, research dissemination, conferences and workshops. CCIS and NorSIS will in collaboration continue to deliver the Top Level Security Meeting which brings together security chief executives for discussions under Chatham House Rule.

Electro Section

CCIS shares campus with the Section of Electronics at GUC. In particular, the Electro Section supports CCIS in a number of security areas, including investigations of electronic equipment in criminal cases, electronic implementations of biometrics methods, combination of biometrics, Near Field Communication and mobile phones, and random number generation in programmable logic. The Electro Section has several associate professors wit PhD degrees in information security.

Health Care and Nursing

CCIS shares campus location at GUC with the Faculty of Health Care and Nursing, which develops expertise in patient safety and security, including information security in the health sector.

FRISC

CCIS works in close collaboration with the Forum for Research and Innovation in Security and Communications (FRISC), a value network supported by the Norwegian Research Council. The mission of FRISC is to create meeting places for research and innovation in information security where information sharing and the value-added utilization of results can happen with an international perspective.

center for cyber- and information security

> There is an opportunity here to establish Norway as the academic centre in cyber security, where innovation and sophistication are the ingredients in dealing with this very complex issue. That's what I think you're starting to establish.

Carlos Solari, former CIO for the White House under President Obama

CCIS' first partners' workshop, November 2013

The Center for Cyber- and Information Security (CCIS) works continually to obtain additional financing for projects and research groups and laboratories.

Delivery

2 years

CCIS will have

-established a research group on cyber crime

-established a research group on cyber defence

-established a research group on cyber security of critical infrastructure

-strengthened and integrated degree programs in information seurity

-started an experience-based master's program on cyber crime investigation

-established the presence of 25 PhD students at the centre and 64 associated via COINS, two post-doctoral candidates, 40 master students and 240 undergraduates

4 years

CCIS will have

-become a strong support for the Norwegian authorities in their national and international work on cyber security

-established a research group in privacy and cyber aspects of rule of law

- establsihed aNordic Centre of Expertise in Cyber Crime Prevention and Investigation

-recruited 30 PhD students at the Centre and with 90 associated via COINS, and 10 postdoctoral candidates

-recuited 25 partners

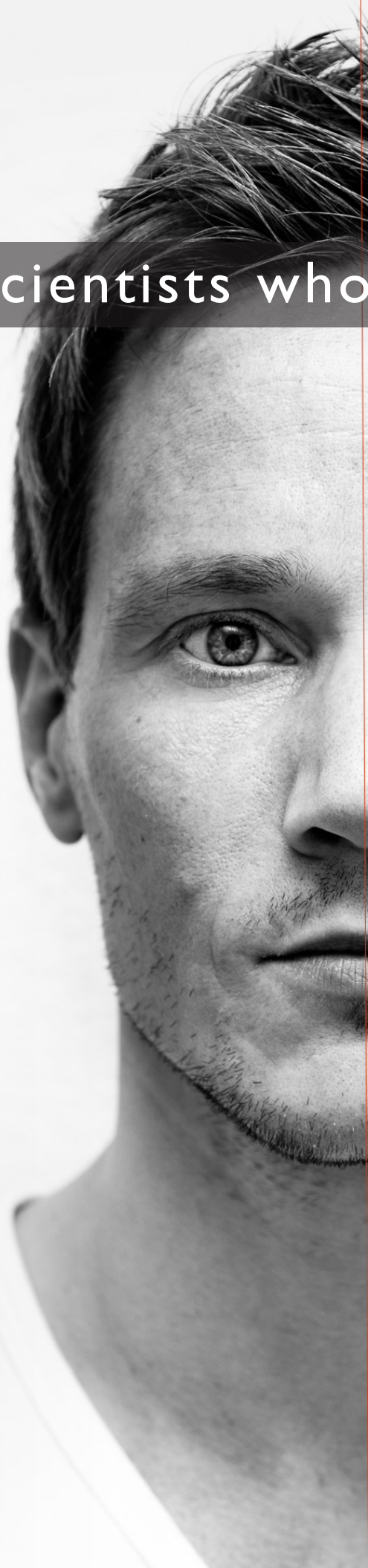
8 years

CCIS will have

-been on track to eliminate society's critical shortage of experts

-led the Norwegian research in cyber security from being fragmented into being a national consolidation of meeting space for the dissemination of research and innovation

-established a centre for cyber security innovation to help industry partners turn the results from CCIS into commercially successful products and services



Scientists who

AT CCIS

50% presence at CCIS
Developing cross-sectoral projects
Developing curricula
Identifying student resources
Developing research networks
Attracting team members

Partner-funded researchers develop the collaboration between CCIS, its partners and networks and the funding partner organisation. "Partner researchers" have the responsibility to help recruiting talented students for partner institutions, influence the development of degree programs in a direction that best supports the partner institution's needs, and connect partner organization to the Centre's other partners and to international networks.

build bridges

AT THE PARTNER INSTITUTION

50% presence at the partner institution

Identifying skills and competence needs

Identifying potential projects

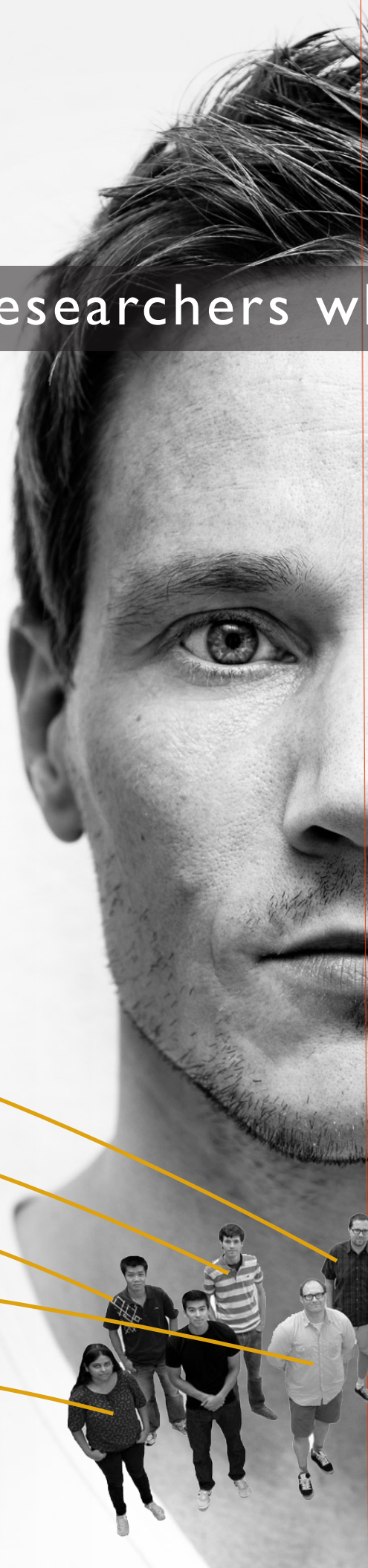
Mobilizing the partner's professional network

Attracting team participants

Partner researchers will support the partner institutions in their long term strategic development, and are responsible for identifying their needs for competence development and research. Partner researchers recruit resources and networks to CCIS projects.

Researchers w

A partner researcher shall draw on resources at the partner insitituion and CCIS to develop a team that will contribute to activities and projects that will further the objectives of the partner and CCIS in the particular focus areas of the partner.
Team members comes from the partner institution, as well as doctoral candidates, researchers, PhD students, master students, bachelor students and experts, at CCIS and among CCIS' partners and their networks. The partner researcher is expected to spend some time doing fundraising and write proposals to finance the team.



ho build teams

CCIS emphasizes good collaboration in an excellent research environment, where social challenges, professional dialogue, and cooperation are central. CCIS focus on eminent research and professional development that connect partner organizations, engineers, security experts, leading expertise and top scholars. It also closely connects applied research, teaching and real world informations security experience and needs. This calls for a good organization that include research groups, focus laboratories, professional groups, and a good cooperation rhytm.

PhD-student

Master student

Domain Expert from partner organization

Technician

MORE REASONS WHY CCIS IS IMPORTANT

6 CCIS is important because society as a whole and its critical infrastructure have become completely dependent on ICT, and therefore dependent on ICT security - from command and control systems, financial structures, food production, food distribution, banking, payroll and electricity distribution to hospital management, and transportation.

7 CCIS is important because the consequences of security breaches have become very high.

8 CCIS is important because inadequate information security costs society large amounts of financial resources. The global cost of cyber crime is estimated to be between 0.4% and 1.4% of global GDP.

9 CCIS is important because an arena for knowledge exchange across information security actors, including defence, law enforcement, police, administration, finance, and business, is necessary for developing effective security capacity.

10 CCIS is important because effective information security measures rely on understanding the security interdepence of technological, economical, legal and political measures.

11 CCIS is important because information security actors, including security agencies and businesses, have much to gain from collaborating with long-term research, while research has much to gain from learning from the so-called "real world".

12 CCIS is important because security has become a necessary part of products and services. Insufficient security can drive products and firms off the market. High cyber security gives manufacturing companies higher uptimes, shorter delivery times and improved margins.

13 CCIS is important because information security in itself is a large global market, both for products and services.

14 CCIS is important because it will give its participants, who have significant national importance, increased cyber- and information security competence.

15 CCIS is important because it will increase the number of students in information security at all levels.

Cyber Security, Information Security, ICT security and Data Security?

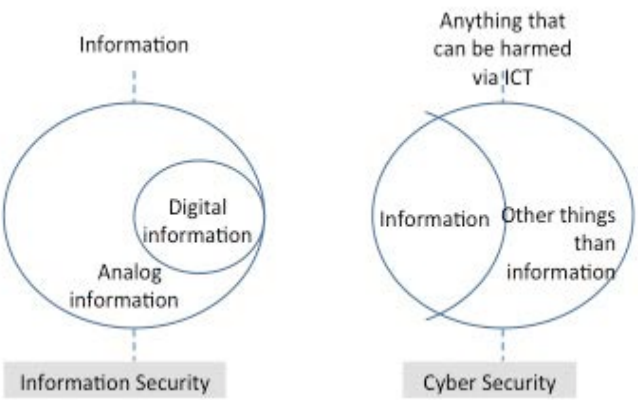
These terms are often used interchangeably, but they do mean different things.

Information security is the protection of information, regardless of whether it is stored digitally or not. Data security and information security for most practical purposes are the same.

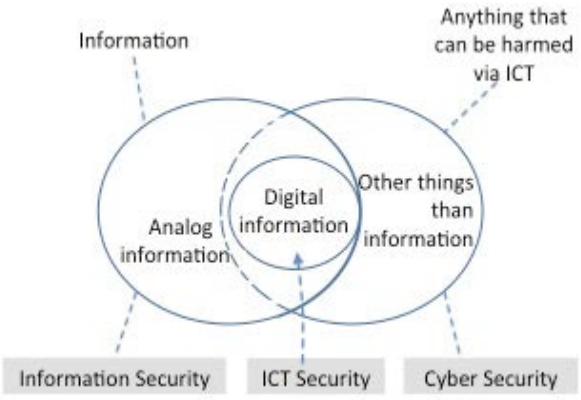
Cyber security is about securing things that are vulnerable through ICT. Let us illustrate the difference between information security and cyber security with the following two Venn diagrams.

The left diagram represents the set of any type of information. This set can be subdivided into digital information and non-digital (analogue) information (e.g. books and notes written on paper).

The right diagram represents the set of things that are vulnerable through ICT. This can be divided into information (both physically and digitally represented) and non-information (such as transformers, medical equipment, vehicles, and traffic lights).



As it is shown below, these two diagrams overlap, showing the relationship between ICT security, cyber security and information security.



ICT security is the protection of information and communication technology, i.e. hardware and software. The reason why ICT security and information security are terms often used interchangeably is that information these days usually is stored and transmitted using ICT. Thus to protect such information, you must protect the technology that stores the information and through which it is transferred. The diagram also shows that even information that is not stored digitally is still vulnerable through ICT (e.g. paper, books in a library, if the sprinkler system is controlled via ICT).

Contact information:

Morten Irgens, Gjøvik University College,
morten.irgens@hig.no, +47 46 54 19 41

Nils Kalstad Svendsen,
the Norwegian Information Security Laboratory
(NISlab), nils.svendsen@hig.no, +47 454 92 425

Thank you for your interest. CCIS is a resource for its partners and collaborators. Your comments and ideas on how CCIS can be made even better will be most appreciated. CCIS invites your organisation to participate as partner.

www.nislab.no

center for cyber- and information security