Næringslivets sikkerhetsråd

The Hybrid Study

Hybrid threats and incidents targeting the Norwegian business community

Conducted by Opinion AS for The Norwegian Business and Industry Security Council

Foreword

Fake news, GPS signal jamming, cyberattacks, election manipulation and destabilisation are words that mark the headlines almost daily. Such measures comprise hybrid attacks targeting society and the business community. In this study, we aim to highlight these challenges, map hybrid incidents and study how the business community understands its role in hybrid warfare.

There are a great number of different ways of which the term hybrid warfare is understood, but there is a broad consensus that it constitutes a serious challenge to the authorities, society and the business world. In the study, we refer to hybrid threats, incidents and operations. These terms comprise hybrid warfare, but in this context, it is more relevant to describe it using other expressions than warfare. The term hybrid refers to agents utilising a broad spectrum of military, political, financial, civilian and information-based instruments targeting civilian society and the private sector.

The hybrid study shall not only map hybrid operations targeting the business community, but also contribute to increasing the focus on the challenges outlined here, and to contribute to preventive efforts. With this study, our aim is to gain insight into how the Norwegian business community sees and understands hybrid threats, how businesses prepare for such threats and how businesses are made a target of hybrid threats and activity.
The Norwegian Business and Industry Security Council is also responsible for the Unrecorded Statistics Study - 2018 and KRISINO - 2017 national studies. This provides very thorough documentation of the business community's security challenges and creates a foundation for further security efforts, also related to preventive and awareness-raising measures in Norway.
We therefore hope that the Hybrid Study will contribute to an increased focus on and awareness surrounding hybrid threats, a greater capacity for detection, as well as preventive security efforts throughout the public and private sectors.

Thank you to everyone who has supported the study.

Jack Fischer Eriksen
Director of The Norwegian Business and Industry Security Council

NSR

NORGES BANK

KPMG

ONE VOICE

mnemonic

DEN NORSKE KRIGSFORSIKRING FOR SKIB
GJENSIDIG FORENING
The Norwegian Shipowners' Mutual
War Risks Insurance Association

VISMA

AkerBP

ONE WORLD

equinor

Special thanks to our contributors: Jan Ivar Botnan, Norwegian Defence Research Establishment, Richard Utne, the Norwegian Armed Forces, Carl-Axel Hagen, Norges Bank and Birgitte Førsund, KPMG.

Contents

Summary

67 percent of businesses with 100 or more employees believe that having a central and well-established position in society makes them potential targets of hybrid threats.

70 percent of the businesses believe a lack of ability to recognise attempts at influencing camouflaged as other inquiries constitutes a condition that makes the business vulnerable to hybrid threats. Furthermore, 63 percent believe lacking security awareness in the organisation makes them vulnerable.
48 percent believe it is unlikely that they will be exposed to hybrid threats, while 24 believe it is likely that they will be exposed to such threats. At the same time, six out of ten believe it is common for businesses in general to encounter hybrid threats.

Computer viruses and phishing operations are viewed as the biggest vulnerabilities that may allow threat agents to gain control of the business's information systems (37 and 27 percent). One out of ten believe that the most likely way a threat agent may gain control of the information systems is if the threat agent exploits employees through blackmail, bribery or social engineering, while 5 percent believe it is most likely that an insider will be placed in the business.

In the event that one encounters hybrid threats, the most serious potential consequences are considered to be the loss of confidential information, interruptions to operations and the loss of reputation.

32 percent of the businesses have noted types of abnormal activity that may comprise a hybrid operation. *At the same time, 14 percent have experienced increased activity during the period the NATO exercise Trident Juncture took place.*
There is no singular answer to who the businesses would contact if they encountered hybrid threats. 63 percent would contact the police, 33 percent the National Security Administration, 28 percent PST, 14 percent NorCert and 12 percent KRIPOS (multiple options could be selected).

About the study

Background

Opinion has conducted the Hybrid Study on behalf of the Norwegian Business and Industry Security Council.

Population

The population of this study is Norwegian businesses in the public and the private sector with 100 or more employees. The selection of this study is drawn from Bisnode's database, which collects information from the Central Coordinating Register for Legal Entities.

354 interviews have been conducted in this study.

Data collection

Data collected was conducted with the aid of telephone interviews (CATI) in the period from 15 November to 04 December 2018.

Error margins

Opinion notes that all surveys entail error margins. The error margins primarily involve statistical uncertainty. There are sampling biases, which prevent the sample from being identical to the universe or to the target population. These differences may relate to certain characteristics or behaviours.

At 354 respondents or interviews (n=354), we can claim with 95 % probability that the exact result is within ± 2.3 and ± 5.2 percentage points, independent of the percentage size. Uncertainty is at its highest at percentage results of 50%, and at its lowest with percentage results of 5% / 95%.

Definition of Hybrid threats and attacks

The definition of hybrid attacks the respondents were given:

Hybrid attacks may include cyber-espionage, influence operations, sabotage and terrorism. What makes these attacks "hybrid" is that they use multiple methods at the same time and that it is difficult to see the connection between them. The agents involved have a greater goal, such as influencing political decisions, exploiting vulnerabilities in society or businesses and a goal of collecting and exploiting information, manipulation and sowing unrest and distrust.

Characteristics

Survey respondents have the following distribution across the private and public sectors:

Sector	Number (n)	Share Interview
Private	187	53 %
Public	167	47 %
Total	354	100.0 %

Geography

Below is an overview of the respondents' location by region:

County	Number Interview (n)	Share Interview
Oslo	58	16%
Eastern Norway in general	126	36 %
Southern/Western Norway	99	28 %
Central Norway	49	14 %
Northern Norway	22	6 %
Total	354	100 %

Business size

The survey encompasses businesses in the following size groups:

Business size	Number Interview (n)	Share Interview
100 to 199 employees	216	61 %
200 or more employees	138	39 %
Total	354	100%

Industry

The survey encompasses businesses in the following industries:

Industry	Number Interview (n)	Share Interview
Industry etc.	52	15 %
Construction and development industries, transport and	40	11 %
storage	24	7 %
Retail, accommodation and food industries	76	21 %
Service industries	33	9 %
Public administration	34	10 %
Education	95	27 %
Healthcare and social services	354	100 %
Total		

1. Businesses as targets of hybrid threats

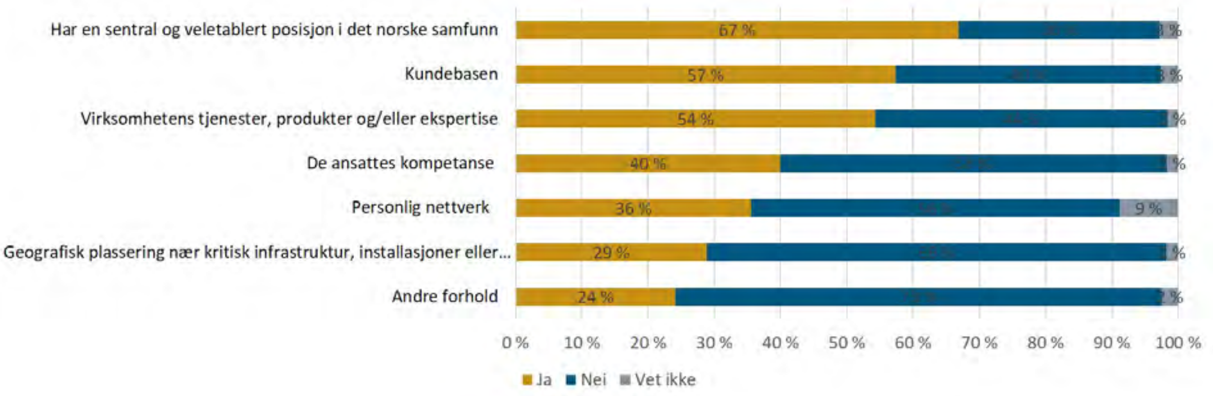
- This chapter encompasses questions related to the businesses' vulnerabilities to hybrid threats and how they understand their role in hybrid operations.

1. Businesses as targets

1.1 Potential targets of hybrid threats

On questions concerning different conditions that may potentially pose a threat to the business, 9 percent believe they are not a potential target of any of the threats. 3 percent perceive all the conditions asked about to be threats that may affect them.

Figure 1 I will now read out some conditions and ask you to answer yes or no as to whether these may potentially make your business a target of hybrid threats. (n=354)



67 percent of businesses with 100 or more employees believe that having a central and well-established position in society is what makes them a potential target of hybrid threats. It is somewhat more common to hold this view in the public sector than in the private sector (76 vs. 59 percent), and businesses in public administration hold this view more specifically. Among businesses that consider themselves part of critical infrastructure, 82 percent believe their central position in society makes them a potential target of hybrid threats.

Nearly 6 out of 10 believe their client base makes them a potential target of hybrid threats. This is a view that is distributed equally independent of sub-group.

When it comes to products, services and/or expertise, 54 percent believe this makes them a potential target of hybrid threats. Businesses that view themselves as part of critical infrastructure (78 percent) hold this view to the greatest degree.

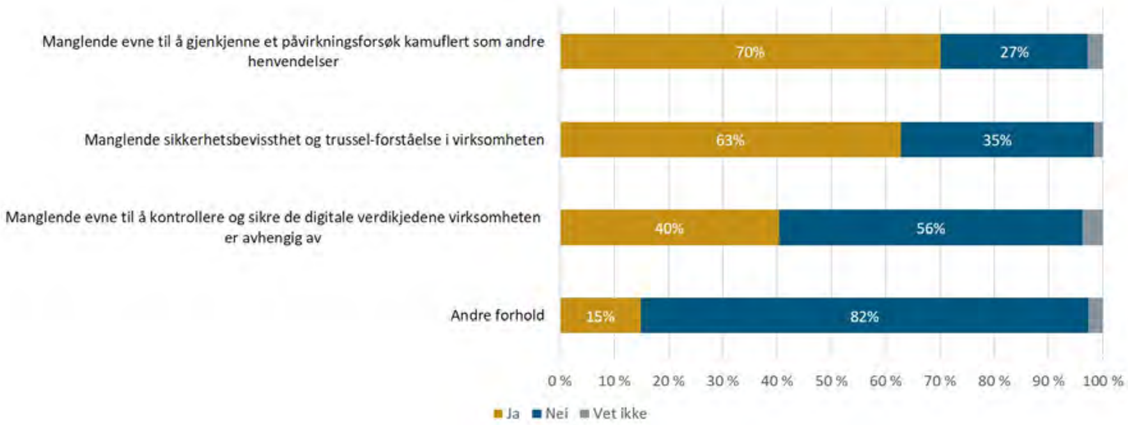
Four out of ten believe their employees' competency makes them a potential target of hybrid threats. This is somewhat more the case in businesses with 200 or more employees than in smaller businesses (48 vs. 35 percent) and among those that are part of critical infrastructure (50 vs. 35 percent).

Personal networks are seen as a possible reason to be a target of hybrid threats for 36 percent of the businesses. Those that are a part of critical infrastructure believe this to a greater degree than others (44 vs. 30 percent). There is no difference for other background variables.

Three out of ten believe geographical location contributes to making them a target of hybrid threats. 40 percent of those who comprise a part of critical infrastructure believe this, compared with 35 percent of others. This is also a more common view in the public sector than in the private (37 vs. 21 percent)

1.2 Conditions that may make businesses vulnerable to hybrid threats
70 percent believe a lack of ability to recognise influencing attempts makes them vulnerable to hybrid threats. Meanwhile, a total of 63 percent believe a lack of security awareness and threat awareness at the business makes them vulnerable to hybrid threats.

Figure 2 Do you believe the following internal conditions may make your business vulnerable to hybrid threats? (n=354)



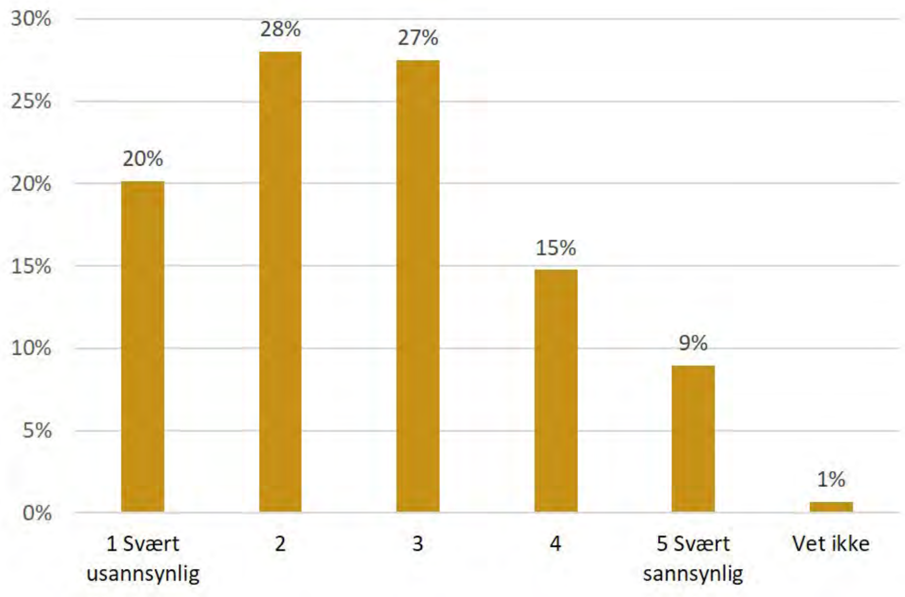
When it comes to a lack of ability to recognise influencing attempts, this is a somewhat more widespread view in public businesses than in private ones (79 vs. 62 percent). There are no differences beyond this. The lack of security awareness and threat awareness as a cause of vulnerability is distributed evenly independent of sub-groups with the exception of it being more widespread in public businesses that belong to public administration.

Four out of ten believe a lack of ability to control and secure digital value chains on which the business is reliant may leave them vulnerable to hybrid threats. Public businesses believe this is the case to a greater degree than private ones (48 vs. 34), but there are no other differences between the sub-groups.

1.3 Probability of being exposed to hybrid threats?

Nearly half believe it is unlikely for them to encounter hybrid threats, while one out of four believe these are likely to happen.

Figure 3 How likely or unlikely do you believe it is for your business to be exposed to hybrid threats? (n=354)

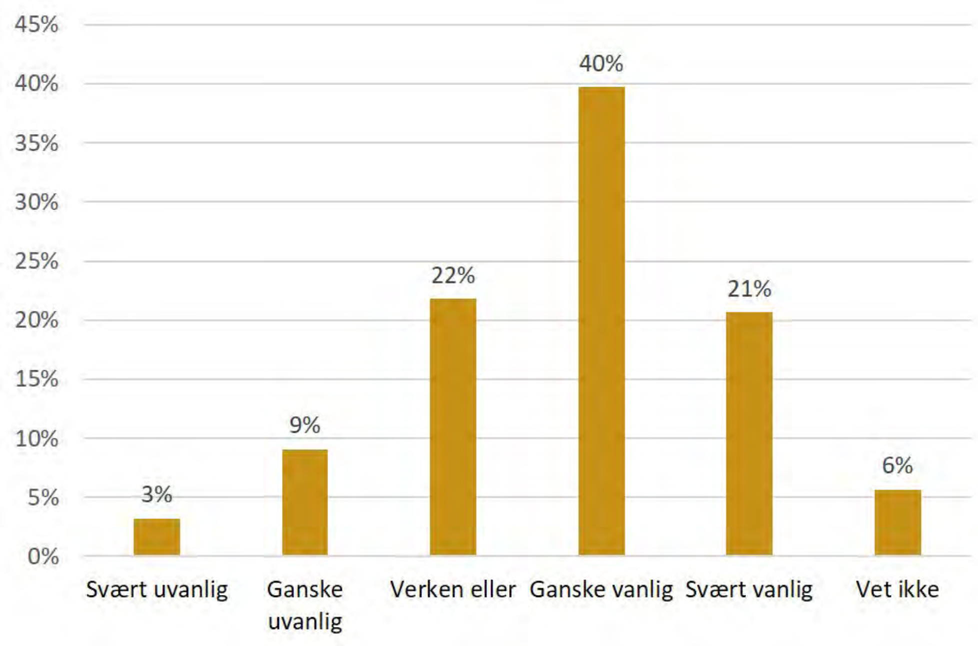


9 percent believe it is highly likely for their business to be exposed to hybrid threats, while an additional 15 percent reply with the value 4 on a scale from 1 to 5. There is no difference between sub-groups, except that businesses in public administration to a greater degree than others believe it is likely to happen, with a total of 26 percent finding it highly likely. However, there is no difference between the public and private sectors.

1.4 Encountering hybrid threats is believed to be common

Six out of ten believe hybrid threats are common, while 12 percent believe they are uncommon.

Figure 4 How common or uncommon do you believe businesses encounter hybrid threats in Norway? (n=354)



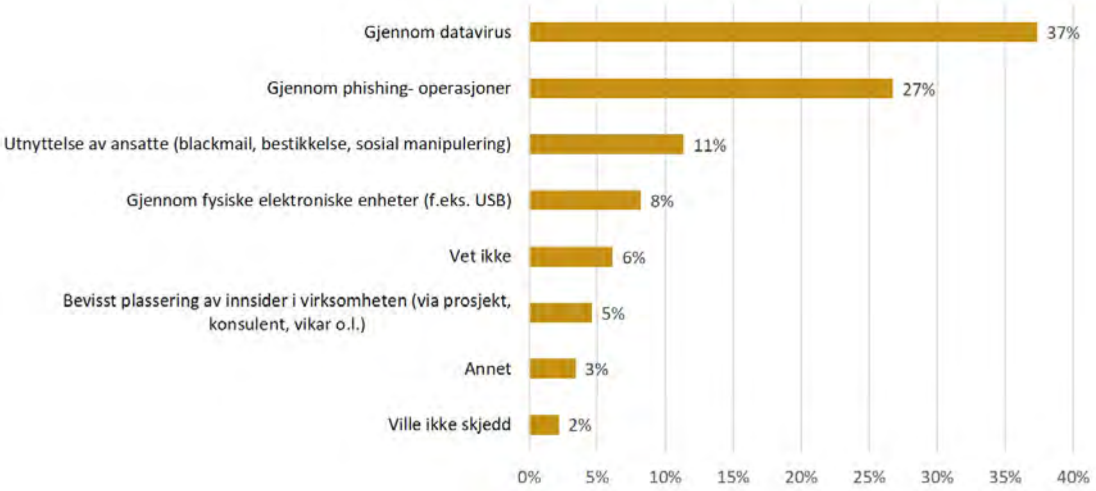
Public businesses in public administration believe to a greater degree that it is common (78 percent reply highly or somewhat common). The same applies to businesses supplying the public sector (71 percent reply highly or somewhat common). Beyond this, there are no differences between different sub-groups.

1.5 Most likely vulnerability

If a threat agent were to access the business's information systems, 37 percent believe this would be due to a computer virus, while 27 percent view a phishing attack as the most likely cause. One out of ten believe exploitation of employees is the most likely method a threat agent may use to gain access, while 5 percent view the placement of an insider in the business as the most likely. Only 2 percent reply that it would not occur.
There are no differences between different sub-groups on this question.

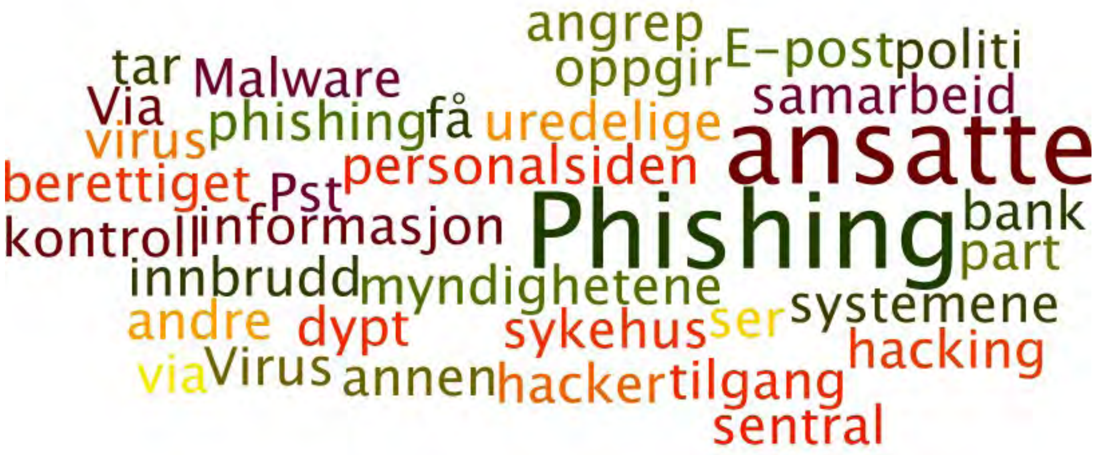
1. Businesses as targets

Figure 5 Imagine a situation in which a threat agent gains access to your business's information systems. How would the threat agent most likely have gained this access? (n=354)



Those who reply other noted conditions such as disloyal employees and incidents occurring through other parties, such as banks.

The word cloud below shows the open answers.



2. Preparation and prevention

- This chapter covers questions related to the business's preventive measures and sources of information.

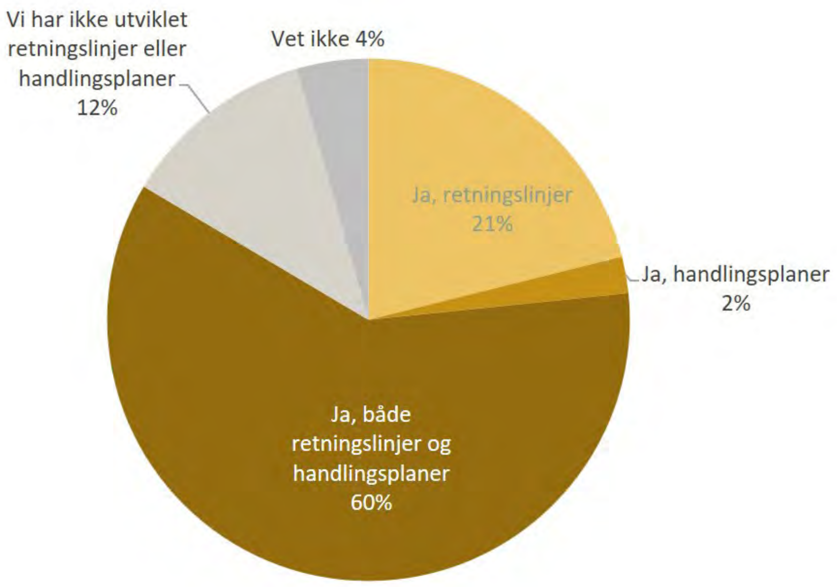
d
urity
ctrl

2. Preparation and prevention

2.1 Guidelines or action plans

Six out of ten have both guidelines and action plans for protecting the business's assets against hybrid threats. 12 percent have not developed guidelines or action plans.

Figure 6 Does your business have guidelines or action plans for protecting your business's assets against hybrid threats? (n=354)



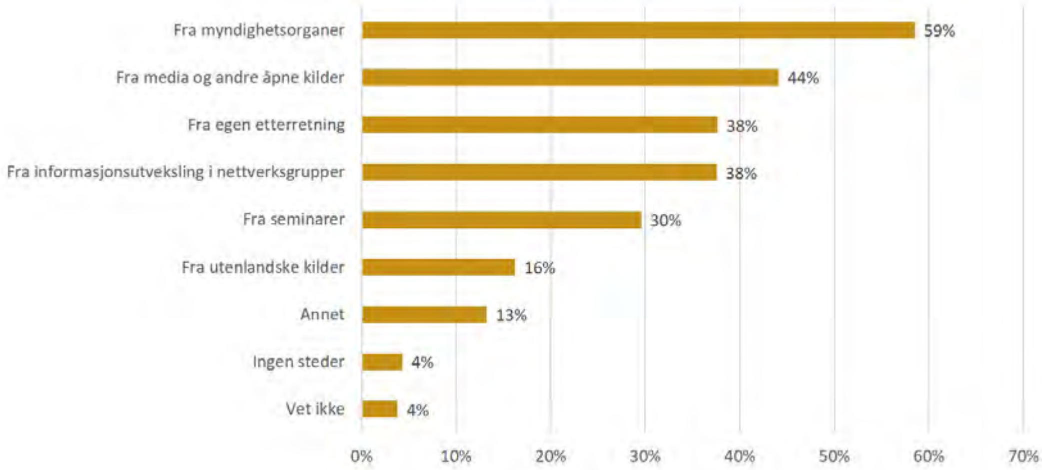
Businesses in the private sector are somewhat less likely to have guidelines or action plans. 16 percent of private businesses do not have such guidelines or plans, compared with 7 percent of public businesses. The condition is approximately the same between businesses that are part of critical infrastructure and those that are not. 15 percent of those that are not part of critical infrastructure do not have guidelines or plans, while 7 percent of those that are part of critical infrastructure are in the same situation.

2.2 Information sources

Public authorities are the most common source of information concerning hybrid threats. Six out of ten receive

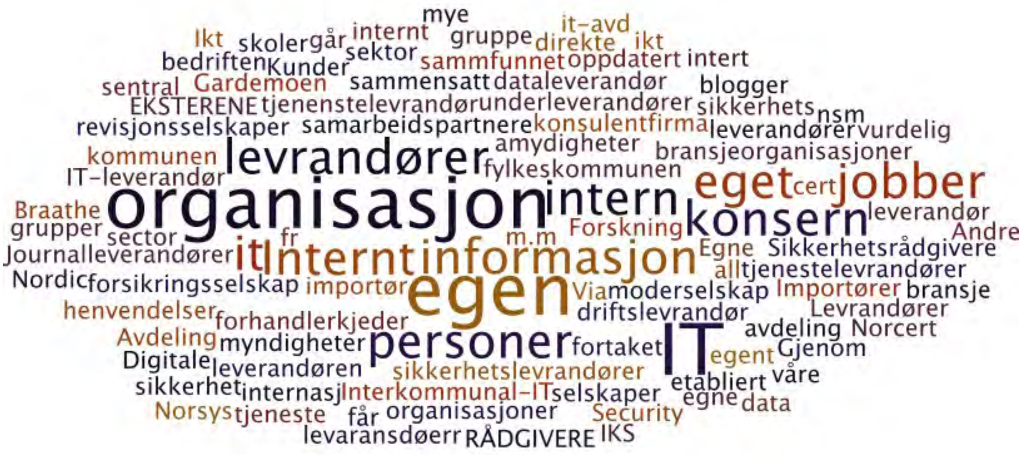
information concerning hybrid threats, operations and activities from this source.

Figure 7 From which parties does your business receive information concerning hybrid threats, operations and activities? (n=354)



Public businesses receive such information from public authorities to a greater degree than is the case for private businesses (67 vs. 51 percent). Private businesses receive information from the media to a greater degree (50 vs. 38 percent) and foreign sources (23 vs. 9 percent) than is the case for public businesses. Those that are a part of critical infrastructure receive information from public authorities to a greater degree than others (68 vs. 53 percent).

Among those who reply with other sources, a series of different possible information sources were reported.



3. Cases and consequences of hybrid threats

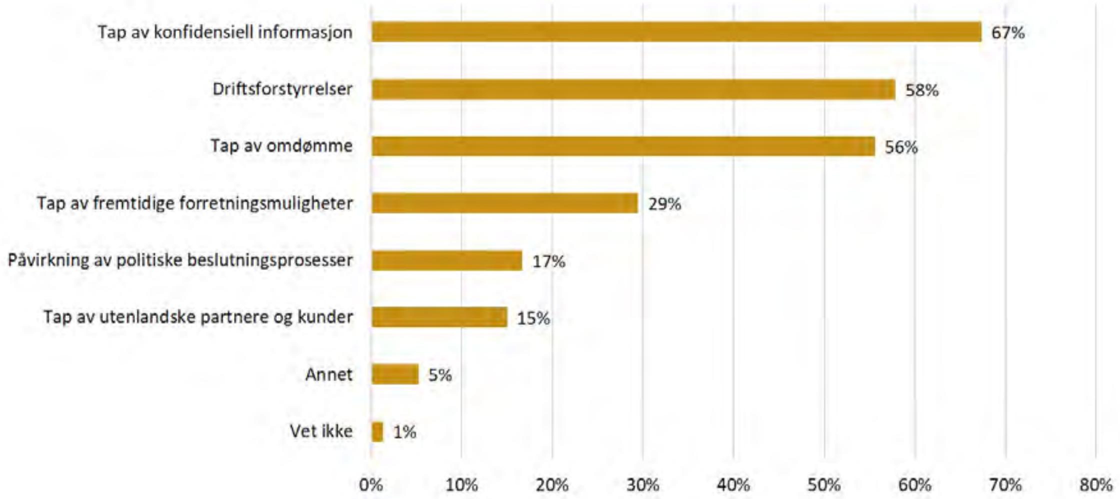
- This chapter maps cases of hybrid threats and deals with questions related to consequences.

3. Cases and consequences

3.1 Consequences

The loss of confidential information is the consequence most imagine to be the result of being exposed to hybrid threats.

Figure 8 What do you view as the most serious consequences of hybrid threats? (n=354)



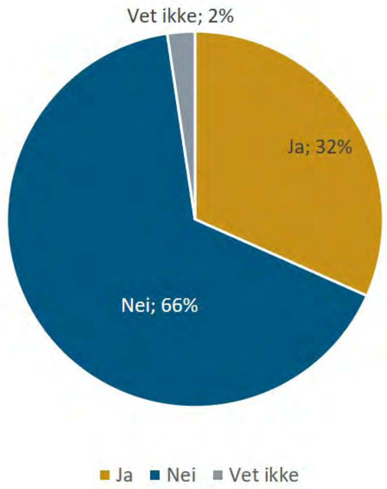
Businesses in the public sector select the loss of confidential information to a greater degree than private businesses (79 vs. 57 percent). The private sector, however, finds to a greater extent than the public sector the loss of future business opportunities and loss of foreign partners as consequences. Those who are part of critical infrastructure see interrupted operations as the most serious consequence. Businesses with 200 or more employees view the loss of confidential information and loss of future business opportunities as a serious consequence to a greater degree than smaller businesses. Businesses in public administration view the influencing of political decision processes as a serious consequence to a greater degree than businesses in other industries (39 percent). The loss of confidential information is put forth as a serious consequence in public administration and in healthcare and social services than in other industries (83 and 79 percent).
Those who have answered other have noted factors such as financial losses as a possible consequence.

Økonomisk
økonomiske
Tap
liv
Økonomiske
LEVEVARNSER
tredjepart/kunder
Fare
forhold
taP
endring
tap
Kundeinformasjon
avveie
transport
helse
info
sabotasje
økonomi
pasientdata
Dødsfall
godkjening
penger
menneskeliv
konsekvens
råvarer
alvorlig

3.2 Abnormal activity

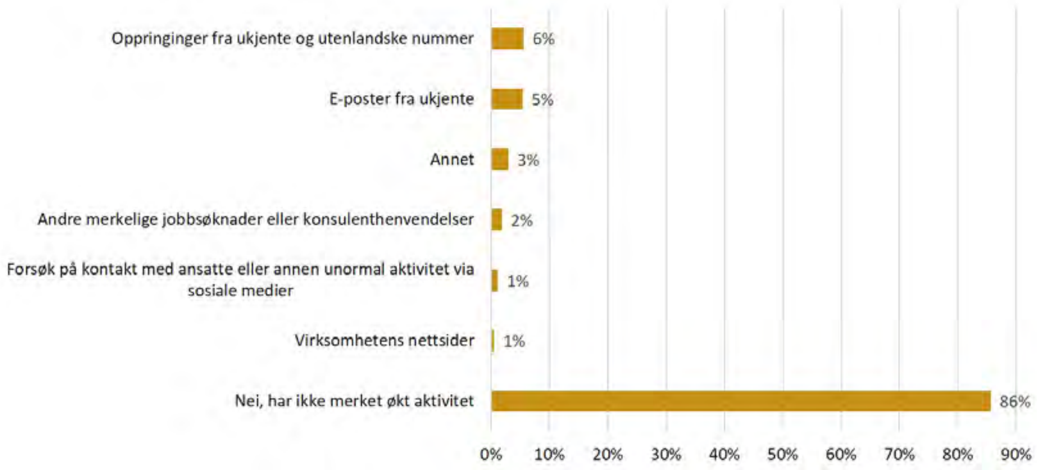
Three out of ten have experienced abnormal activity that may comprise a hybrid operation. There are no differences between businesses in different sub-groups on this question.

Figure 9 Have you discovered any kind of abnormal activity directed at your or someone else's business that may comprise a hybrid operation or a part of such an operation? (n=354)



While 32 percent have experienced abnormal activity directed at their business at some point, 14 percent state that they experienced increased activity that may comprise hybrid threats during the period in which the NATO exercise Trident Juncture took place (selecting one or more of the options below).

Figure 10 The NATO exercise Trident Juncture was conducted in Norway in fall 2018. Did your business notice increased activity in the following areas in this period? (n=354)

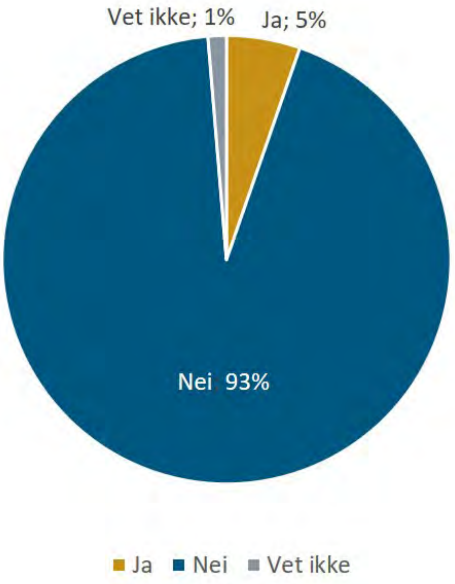


3. Cases and consequences

Among those who experienced activity during the period in which the NATO exercise took place, calls and e-mails were the most common. Respectively, 6 and 5 percent of businesses experienced these. A further 2 percent encountered unusual job applications and consultant inquiries, while 1 percent encountered attempts to contact employees through social media, as well as activities targeting the business's website.

5 percent of the businesses have heard of other businesses in their network being exposed to increased activity that may comprise hybrid threats during the period in which the NATO exercise took place.

Figure 11 Have you heard of others in your network who have experienced increased activity in the listed areas during this time period? (n=354)



There are no differences between businesses in different sub-groups when it comes to the questions concerning activities during the NATO exercise.

4. Cooperation against hybrid threats

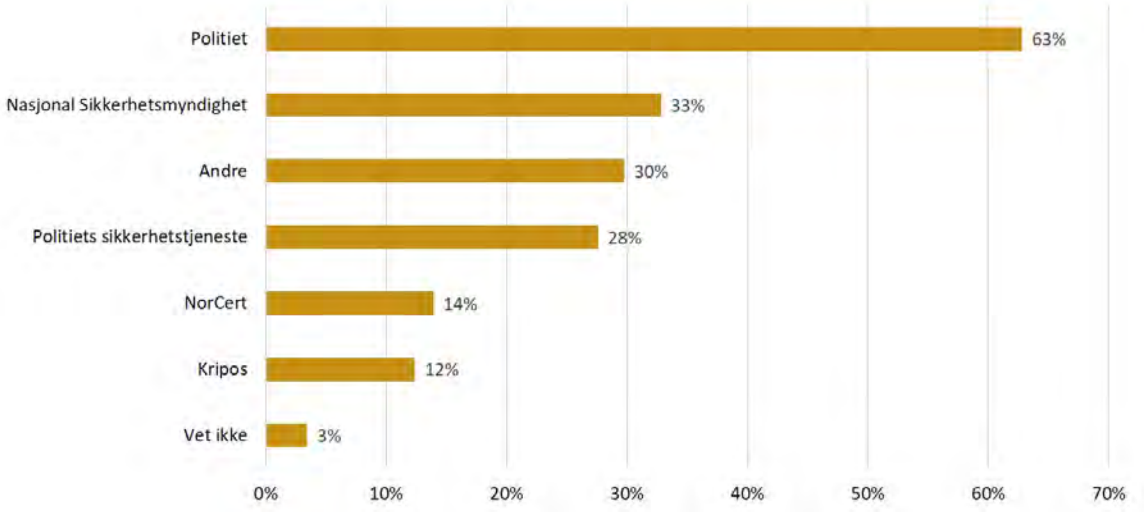
- This chapter deals with the reporting of hybrid threats and expectations to the authorities.

4. Cooperation

4.1 Which public authorities are contacted

If one encounters hybrid threats, businesses will first and foremost contact the police.

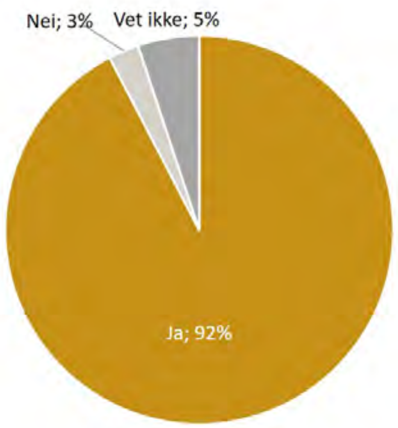
Figure 12 If your business were to encounter hybrid threats, which public authorities would you contact? (n=354)



63 percent would contact the police if they encountered hybrid threats, while a relatively large share would also contact other parties.

A major part of the businesses will share information with Norwegian authorities if suspicious activity targeting the business is discovered. This is a stance that prevails independent of sub-group.

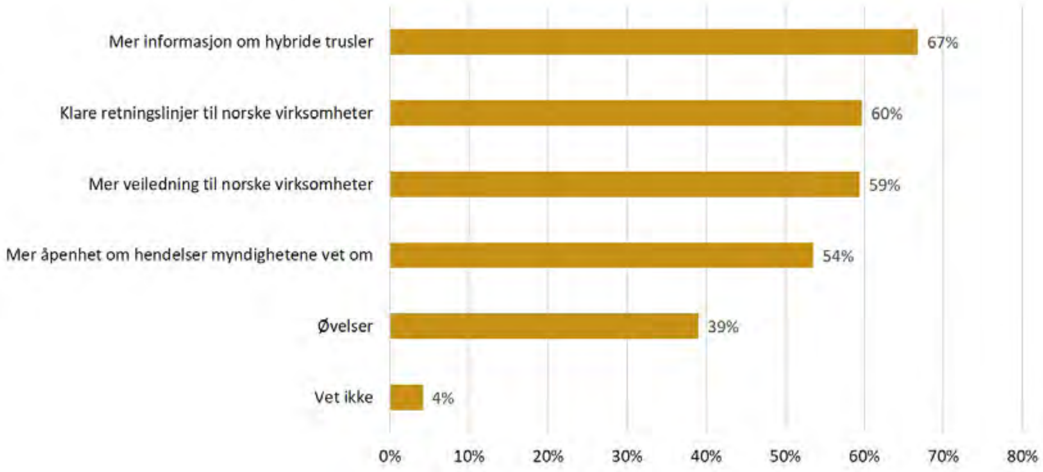
Figure 13 Would your business share information with Norwegian authorities if suspicious activity targeting the business were discovered either in a different country or in Norway? (n=354)



4.2 Disclosing hybrid threats

More information from the authorities concerning hybrid threats are requested by the authorities.

Figure 14 Of the following options, which do you believe Norwegian authorities should contribute with to disclose hybrid threats? (n=354)



67 percent request more information concerning hybrid threats. Otherwise, it is worth noting that 54 believe greater openness concerning incidents the authorities are aware of will be a good disclosure method. This applies in particular to businesses with 200 or more employees, as well as the construction/development and transport industries (63 and 76 percent, respectively).

5. Loss of resources

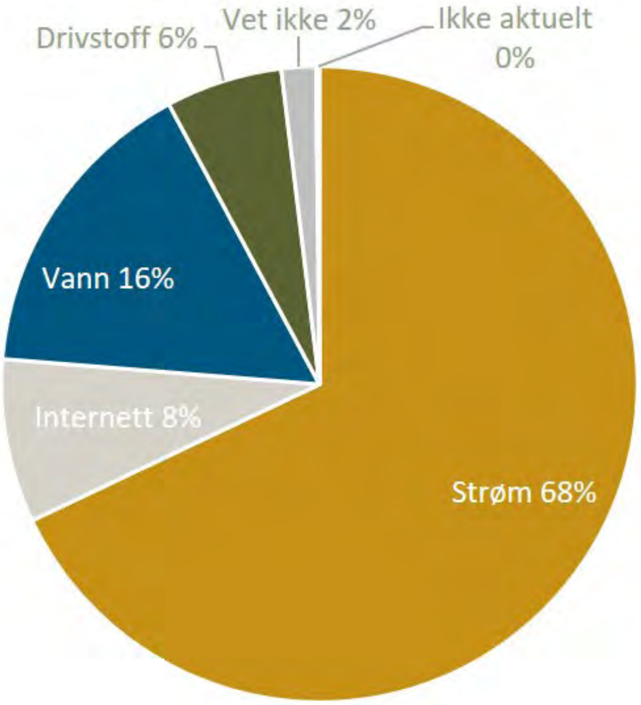
- This chapter examines the businesses' ability to withstand disruptions to access to resources.

5. Ability to withstand disruptions

5.1 5.1 Loss of resources

If power, internet, water and fuel are unavailable, the loss of power will be noticed to the greatest extent.

Figure 15 Imagine that power, internet, water and fuel are unavailable. Which of the four would have the biggest impact on your business? (n=354)



Businesses in construction/development and transport naturally believe to a greater extent that the loss of fuel will have the biggest negative impact (33 percent). Businesses in public administration believe to a greater degree than others that the loss of internet will be serious (22 percent), while the loss of water will be the most noticeable in education as well as healthcare and social services (26 and 34 percent).

6. Analysis

In this chapter, we have analysed some of the findings in the study.

6. Analysis

6.1 Hybrid threats – common, but unlikely?

Businesses that believe it is common for businesses to encounter hybrid threats in Norway view it as unlikely for them to be affected themselves.

A high percentage of respondents, 60 percent, believe it is common for businesses to encounter hybrid threats. Meanwhile, 48 percent report that they believe it is unlikely for their own business to encounter hybrid threats. This trend can be seen across sectors, geography, and the size of the business.

The findings thus point out an interesting tendency; the business community views it as common to encounter hybrid threats, while at the same time believing the probability of something happening with their own business to be low. This may suggest a common perception that hybrid attacks are something distant and unthinkable. There is a lack of clarity and consensus surrounding the term hybrid attack. The term is presented and applied differently in different industries, environments and areas. An assumption is that most believe that hybrid threats are incidents that draw a lot of attention and that, without a doubt, are perceived as an attack by all involved parties. However, experience shows that incidents may be small and difficult to discover, and may take the form of mapping, cooperation, taking initiative to make contact and attempts to influence.

For businesses reporting that they are part of critical infrastructure, 67 percent report that they believe it is common for businesses to be exposed to hybrid threats. At the same time, 48 percent report that they view it as unlikely for their own business to encounter hybrid threats. Non-attributable cyber-operations[1] targeting public services and infrastructure are presented by FFI as one of the most important challenges the authorities may stand before in the event of a hybrid attack.

It may be challenging to see how hybrid threats may affect or challenge one's own industry. In public administration, 78 percent believe it is common for businesses to encounter hybrid threats in Norway. A further 48 percent report that they believe it is probable for their own business to encounter hybrid threats. One possible explanation for the focus from this specific industry may be that they are controlled by political processes and are thus informed about the threats they may face to a greater degree.

6.2 The business’s position in society – does it play a part?

Trust is a key variable in protection against hybrid threats. Social trust promotes a sense of security and contributes to cooperation and coordination. Social trust means that people trust each other, the structures of society and the authorities. This readies our ability to prepare and protect several critical functions and daily operations. This is precisely why trust is a target of hybrid operations[2].

Businesses with well-established positions in society therefore often hold a large amount of trust from the population. The study shows that 67 percent of respondents report their central and well-established position in Norwegian society as a condition that may potentially make their business a target of hybrid threats. For example, an attack on the computer systems of a hospital will be a part of an attempt to weaken the population's trust in a highly important institution.

[1] Non-attributable attacks mean the agent behind them is unknown, making a counter-attack impossible (FFI Report 18/00080)

[2] (HyWbrid CoE, 2018).

From the public sector, 76 percent reply that their central and well-established position in Norwegian society is a condition that may potentially make the business a target of hybrid threats. From the private sector, 69 percent from industry, 62 percent from construction and development and 59 from the service industry report that their central and well-established position may potentially make the business a target.

For businesses that are providers of critical infrastructure, 78 percent report that the business's services, products and/or expertise makes the business a potential target of hybrid threats. This may indicate that the businesses understand that their business is an attractive target of threat agents. Surprisingly, 48 percent from the same group report that they view it as unlikely that their own business will encounter hybrid threats.

Respectively, 91 percent and 83 percent in public administration report the business's services, products and expertise, as well as the employees' competency as conditions that may potentially make them targets of hybrid threats.

6.3 Weak security culture – a vulnerability?

A perception may be that hybrid activity only takes places at a state level; with one state influencing the stance of a different state. By studying the various means hybrid operations can utilise, it is clear that the population, local community and business community play a significant role both as targets and in the role as a good force for prevention with the aid of a strong security culture.

83 percent of respondents from public administration report that the employees' competency may potentially make the business a target of hybrid threats. The findings are interesting when compared with The Norwegian Crime and Security Survey (KRISINO) 2017, which shows that only half of Norwegian businesses conduct an identity check in conjunction with hiring processes, and approx. 30 percent conduct verification of diplomas. A disloyal servant can easily exploit and abuse the competency of the employees. In this year's study, questions were also asked about how a threat agent most likely would have gained access to the business's information systems. 5 here replied through the conscious placement of an insider in the business (such as through a project, consultant services or substitute).

The study also shows that 70 percent believe a lack of ability to recognise an attempt at influencing may make the business vulnerable to hybrid attacks. At the same time, 63 percent believe a lack of security awareness and threat awareness in the business constitutes a vulnerability. In public administration, a total 96 percent report that a lack of ability to recognise an influencing attempt may make the business vulnerable to hybrid threats and 91 percent believe a lack of security awareness and threat awareness may make the business vulnerable to threats. In the Unrecorded Statistics Study 2018, 39 percent reported that a lack of security awareness among employees was a reason security breaches occurred. This shows that the conditions the business community believes makes businesses more vulnerable are in fact accurate. It is furthermore interesting to compare with numbers from KRISINO 2017, in which only 16 percent stated that they read PST's threat assessment, and only 11 percent read NSM's risk assessment. This sends a strong signal for what should be improved and for what is an individual measure.

40 percent report that a lack of ability to control and secure the digital value chains on which the business relies may be a condition that leaves them vulnerable to hybrid threats. In the Unrecorded Statistics Study 2018, 8 percent report that problems caused by outsourcing partners were a reason security breaches occurred.

6. Analysis

On questions concerning how a threat agent would most likely gain access to the business's information systems, 37 percent report that it would be through a computer virus, and 27 percent through phishing operations. The Unrecorded Statistics Study 2018 confirms this assumption and indicates that viruses or malware infections are the most serious incident that can occur. Phishing operations exploit and deceive persons in businesses, and the incidence of these has increased sharply from 2016 to 2018.

6.4 Severe consequences

When it comes to the most severe consequences of hybrid threats, the loss of confidential information is the one reported by most as the most severe. From there, interruptions to operations at 58 percent, and loss of reputation at 56 percent, are viewed as the most severe consequences.

17 percent of responders report the influencing of political decision processes as one of the most severe consequences of hybrid threats. From the responders in public administration, 39 percent view the influencing of political decision processes as one of the most severe consequences. This is alarming as an influencing operation may result in immense consequences and may put fundamental democratic principles in jeopardy.

6.5 Incidents

32 percent of responders have encountered some kind of abnormal activity directed at their or someone else's business that may comprise a hybrid operation or a part of such an operation. 40 percent in industry, 42 percent in public administration and 37 percent in education answered yes to this question. The findings are particularly notable in Northern Norway, where 40 percent report that they have experienced abnormal activity. *This indicates a geo-political tension that is worth bearing in mind during the term of the Municipal and*

County Board Elections in 2019.

The NATO exercise Trident Juncture was conducted in Norway in fall 2018. The study shows that 14 percent of respondents experienced increased activity or inquiries during this term. This highlights the fact that the threat profile may change in keeping with our own activities. This is a situation that is important to signal to the authorities, the business community and society in general.

6.6 About the cooperation between the authorities and the business community

On the question concerning which public authority a business would contact in the event of a hybrid incident, 63 reply that they would contact the Police, while 33 percent state that they would contact NSM, 30 percent state "other" and 28 reply PST.

The answers show that it is not unequivocal for the business community who they will contact when they encounter something suspicious that may be related to a hybrid incident. For many, the "police" or responsible authority are experienced as fragmented, and it is unclear who is responsible for what.

From having one police force with a clear national mandate, developments in technology and the digitisation of society over the past ten years have given us a social structure and organisation of specialised units that are subject to various departments and public authorities. Certain public authorities may also have overlapping functions, and the division of responsibilities may therefore be unclear for the business community and society.

"The NATO exercise Trident Juncture was conducted in Norway in fall 2018. The study shows that 14 percent of respondents experienced increased activity or inquiries during this term."

6.7 Sharing of information between authorities and the business community

On the question of which information sources business community agents receive information on cyber-attacks from, 59 percent reply that they get this from the authorities by various means, 44 percent reply the media, and 38 percent state that they receive necessary information through their own investigation. In our digitised society, information and competency in security have become a required fresh product.

In addition to the amount of information being digitised, there are furthermore no limits to access to all types of technology, meaning that the authorities do not always have a "technology step ahead" over criminals. Together this means that all of us, in business, the authorities, police and armed forces must remain up to date on the threat profile 24/7 and share more of own incidents, investigations and experiences than ever before.

On questions of whether the businesses are willing to share information with the authorities, a total 92 percent reply that they do, 3 percent reply no and 5 percent reply "don't know". That there is such a large share reporting that they wish to share information with the authorities corresponds with the fact that nearly 90 percent of digital infrastructure in Norway is in private hands. *It also shows a desire from the business community to take responsibility and cooperate in a better manner than is the case today.*

On the question regarding more information from the authorities concerning hybrid threats, 76 percent report that they want more information, 60 percent desire more guidelines, 59 percent want instructions and 54 percent want more openness from the authorities.

A positive development is that the Norwegian Intelligence Service has been publishing open threat assessments over the past 3 years. The dissemination of information for concrete and appropriate measures is a challenge that has not been adequately solved as of this writing. According to the Crime and Security Study in Norway – 2017 (KRISINO) under the direction of the Norwegian Business and Industry Security Council, 14 percent in the private sector had read PST's threat assessment, compared with 26 percent in the public sector. The equivalent figures for the NSM risk assessment are 8 and 21 percent, respectively.

6.8 Cooperation between civilian institutions and the armed forces

The divide between the military and civilian sectors is gradually eroded through digitisation. A hybrid attack may come from a state agent, organised crime, terror organisations or through an individual. Alternatively, there may be a criminal organisation conducting cyber-attacks for a state agent. Hybrid attacks may be targeted at the vulnerable sides of society, particularly through digital vulnerabilities. Therefore, new thinking is needed in vulnerabilities, rather than focusing entirely on critical infrastructure.

Hybrid threats require proactiveness and coordination across sectors, departments and areas of responsibility. It also requires an anchored and shared understanding of the situation.

7. Hybrid measures

- This chapter deals with developments, occurrences, definitions and experiences with hybrid measures.

7. Hybrid measures

7.1 Hybrid measures - an unforeseeable threat

Jan Ivar Botnan, chief researcher, Norwegian Defence Research Establishment

Introduction

In 2018, the NATO exercise Trident Juncture was conducted with great involvement from parties in both the military and in civilian society. The cooperation between several sectors within the framework of the revitalised Total Defence was exercised in light of the allies' needs, regulations and threat profiles. The exercise has been judged a major success, but the total defence concept itself raises several important questions that must be afforded attention in further efforts with the country's readiness. When the Norwegian Armed Forces, through use of the readiness acts and readiness agreements makes use of civilian providers for their operations, these may become legal targets of war. Furthermore, critical civilian infrastructure may be attacked during a crisis or war to weaken readiness and the will to resist political pressure. These are known methods from war history. Public and private businesses that contribute to maintaining critical societal functions may be exposed to espionage, sabotage and terrorism. The terror bombings of England in 1940 and of Germany in 1945 are examples of this, even though the goal of the bombing was not achieved; the will to resist was not weakened, on the contrary, the opposite happened. This shows that it was difficult to predict the psychological consequences of an attack against a society, which was also shown by the reactions after 22 July 2011. The country came together in solidarity rather than hunting for someone to blame.

In this year's threat assessment from PST, it says: "Government-run network operations represent a persistent threat against Norwegian assets. The methods are cheap, effective and in constant development, and attackers are constantly finding new vulnerabilities they can exploit." This is correct, but in order to be useful to daily readiness efforts, this statement must be made more nuanced and concrete.

We must clearly work in a structured manner to establish a broad readiness against malevolent actions from terrorists and foreign powers. This will naturally occur in cooperation with allies and close friends, but history shows that even our closest may distort reality for political reasons. Therefore, there is no alternative to national competency.

Russia's pattern of operations in Ukraine has put the term hybrid warfare on the agenda in our readiness planning. Although hybrid warfare is not something new in principle, social developments and the threat profile have opened for new, and previously unknown challenges in the civilian sector. It is therefore beneficial that the Norwegian Business and Industry Security Council has mapped the understanding and experience of hybrid attacks. As an introduction, we shall note that 67 % of the respondents desire more information on hybrid threats, and that 54 % believe the authorities must show more openness concerning incidents that have taken place.

Hybrid warfare

The term hybrid warfare was introduced in 2007 by Frank Hoffman. He analysed how the Taliban, Al-Qaeda and Hezbollah made progress against conventionally stronger opponents and termed their successful operations as hybrid warfare.

Russia's operations in Ukraine in 2014 were surprising and put the term hybrid warfare on the agenda in earnest. During their annexation of Crimea and support for the revolt in Donbass, violations of international law, Russia conducted sabotage, spread false news that resonated with the ethnically Russian population, and used irregular forces. This proved to be highly effective, and Russia took control of Crimea with minimal use of traditional military force.

Experiences in Donbass were more mixed. The operations stood in stark contrast to the wars in Chechnya and Georgia, which were unnecessarily violent, conducted using old materiel and under poor management.

It was claimed that Russia had developed a new strategic concept (hybrid warfare) that was to compensate for the country's inferiority to NATO in terms of conventional military forces. Support for this claim was found in an article by General Gerasimov from 2013. Gerasimov does not use the term hybrid warfare, however. His article is about how effectively the West has toppled ruling regimes without the use of military means. His examples are the Arab Spring (2010-11), the Orange Revolution in Ukraine (2004) and the Rose Revolution in Georgia (2003). The article is built on a lecture he held for military leaders he accuses of not having "paid attention in class". Gerasimov may be correct in some of his analyses, but he exaggerates, particularly when it comes to parts of the Arab Spring where the Americans showed little interest in supporting the democratic movements, and were criticised for this as well. At the same time, the concept of hybrid warfare itself, or the use of hybrid measures, should be afforded some attention. In a future conflict, we must be prepared to be exposed to all relevant measures an opponent presides over, including nuclear weapons, that admittedly are difficult to include under the definition of hybrid warfare. In particular for the operations in Ukraine, Russia could play on the country's history, the deposition of the legally elected president and the large Russian minority that felt itself discriminated by Kiev. Such conditions will not be found in Norway, but there are good reasons to believe that the Baltic countries, with significant Russian minority populations, will feel uneasy. In these countries, there are reports of attacks on infrastructure without these being followed up by other measures.

Hybrid measures may be effective. It is the task of the intelligence and security authorities' role to monitor the exercises of other countries, map capacities and their own vulnerabilities, and to assess which new technologies may be used. To illustrate the range of hybrid measures, a few examples will be given. The foundation should be that an opponent will consider all options.

In the last decade, there has been explosive development in biotechnology. The human genome has long since been sequenced, and new options for the influencing of life processes have been developed in the service of research and medicine. In this, however, there is also a new threat. During the cold war, biological weapons were built on naturally occurring micro-organisms. Micro-organisms can now be genetically modified, allowing them to cause hitherto unknown illnesses and, for instance, to be resistant to available vaccines and antibiotics. New drugs that have a dulling effect and affect judgement are under constant development. It is not difficult to imagine that such measures may be used to weaken readiness by putting key personnel out of function. This may be easier than physically knocking out a power supply network, blowing up a bridge or hacking into the process management system of a terminal for gas exports. Unfortunately, little has been done about this threat; it is easier to deal with bullets and explosives.

One measure that has received a lot of attention in the form of official investigations and reinforcement of expert communities, however, is cyber-attacks. Investments in better counter-measures are necessary in light of rapid technological threat development. New and more effective systems have been introduced without security with regard to cyber-attacks having been sufficiently improved. Many communities are now actively dealing with this, but security gaps and inadequate organisational security continue to be discovered.

7. Hybrid measures

This invites criminal attacks that cause major losses for the business community. It is therefore natural to add significant resources to protect their own business. In certain businesses, close cooperation is done with industry CERTs with support from national resources.

The question in this regard is whether hybrid attacks are also conducted or planned against central private and public businesses. The purpose in this case will be to weaken Norwegian society in crisis and war. Here, we find a problem: How do you distinguish such attacks from crime and advanced "pranks"? Those who work with hybrid measures may also be interested in espionage for purely financial motives. In practical security efforts, it may make no difference what the motive is, and protecting oneself is important regardless. However, it remains a fact that the groups that prepare hybrid warfare under the direction of governments are highly skilled and have a strong supply of resources. They can operate in a manner that makes it nearly impossible for individual businesses to recognise and avert attacks. Therefore, we must have strong national resources that can support security efforts in the most exposed industries, as the Security Act stipulates.

It is important that the national threat profile is calm and balanced. Only the opponent gains from negligence and exaggeration. Many businesses in Norway are well-secured, making it extremely difficult to intrude and take control of the process control systems. In open literature, there are very few well-documented examples of this taking place. One extreme exception is Stuxnet, the computer virus that caused Iran's centrifuges for uranium enrichment to run amok. However, this was a highly resource-intensive operation, one which the most advanced states were behind, with several years spent on development. It is unlikely that anyone will prioritise such efforts for anything but the most high-priority targets. This understanding must be reflected in readiness efforts.

For understandable reasons, businesses are not very open about security incidents, in part not to seem like easy targets and in part to avoid weakening the trust of the stock market. Nonetheless, knowledge concerning incidents is the most important foundation of good readiness. Therefore, more work is needed for more systematic reporting of incidents so that they can be included in the basis for the security authority's advice. More openness concerning incidents is desired by 54% of the study respondents.

The Hybrid Study is a good addition to the otherwise good work being conducted to protect Norwegian businesses from cyber-attacks, including defence against hybrid measures. However, there is one element in the threat profile that should be afforded more attention: social media. The most successful hybrid attack is when one can achieve one's goals without the use of military resources. For example, Swedish opinion may, in a future referendum on NATO membership, be influenced by a foreign power. This has clear parallels to what may have taken place during the presidential elections in France (2017) and the USA (2016), as well as in the Brexit referendum in the United Kingdom (2016). This type of influencing is not something new; propaganda has been used in most conflicts. What is new is that the internet and especially social media gather enormous amounts of personal information for promoting the sender and entertainment for their circle of friends. Some of this may also be illegal or at least unpleasant for the person involved.

Election influencing

The ultimate impact of hybrid measures is to change the outcome of democratic elections. This is most efficiently completed in cooperation with political groups whose interests align with foreign powers or who for other reasons see a benefit in gaining support from outside. During the Cold War, several political parties in Western Europe received financial support from Moscow.

A noticeably more aggressive Russian foreign policy has again placed the issue of influence on democratic elections on the agenda. First of all, there has been suspicion of involvement in the USA presidential election and the Brexit vote, both of which gave unexpected results. Later, there was concern that Russia would actively influence the elections in Germany and France (2017), in particular because the advancement of Eurosceptical parties would be in Russia's interests. In the wake of the refugee flow from Syria, conditions were right for incidents of violence, one-sided news focus, the spread of compromising information and fake news would influence large groups of voters.

The American presidential election

Let us return to the Western interpretation of General Gerasimov. The purpose of hybrid measures is to achieve political goals at the lowest possible price, preferably without being revealed and with minimal use of power and losses. From the Western side, Russian operations in Ukraine are used as frightening examples of the Russians having learned quickly, and have the will and means to attack their neighbouring countries. Once the dust has settled in Washington, and hopefully all the conditions surrounding the presidential election in 2016 are on the table, Russian coordination with certain American politicians and the theft of sensitive information may appear to be the ultimate example of successful use of hybrid measures, a case study for anyone planning the same.

After the presidential election in USA in 2016, the Americans have withdrawn from international agreements and cooperation, thus allowing countries like China and Russia to strengthen their positions. The president has signalled a reduced American presence in the Middle East, and has at times sown doubt about the relationship with NATO. At the moment, the relationship between President Trump and many of his European allies is cool, while he appears to have a far more positive relationship with President Putin, Chairman Kim Jong-un, Crown Prince bin Salman and Prime Minister Netanyahu. Conflicts can come from this. From Moscow's point of view, these could be seen as excellent opportunities to recreate the status and influence of the Soviet era.

How could this happen; are the Russians extremely skilled or has the development of society and access to new measures made it easy? With our own readiness in mind, it will be useful to recap the incidents surrounding the presidential election as we know understand them.

In 2016, the USA was a polarised society. Middle-class Americans felt forgotten by the Washington elite, who were seen as maintaining their interests through the payment of enormous salaries and bonuses. The use of federal funds to save the banking and automotive industries during the financial crisis of 2008 was seen as a betrayal of everyone who lost their homes. While the parties in congress were previously able to reach a compromise in difficult matters, the fronts were at a standstill. The will to compromise was punished hard by core voters. This was the backdrop for Trump's successful campaign. His behaviour during and after the election has contributed to further polarisation.

7. Hybrid measures

President Trump quickly came into conflict with the power structure of Washington. He had a shaky relationship with the truth. A count by the Washington Post shows that he in 2018 lied 15 times a day (in the public space). When the president sets such a standard, it is easier to make progress with fake news that may serve the interests of a foreign state. The border between truth and lies is blurred. Trust in the holders of power is weakened.

American intelligence agencies concluded in January 2017 that the Russian government had influenced the American presidential election by intruding into the computer network of the Democratic Party and stealing the personal e-mail of Hillary Clinton's campaign manager John Podesta, to then disclose it to WikiLeaks. Furthermore, they had spread fake news on social media and attempted to breach election systems and databases in several American states. These claims were confirmed by Dutch intelligence, which is claimed to have followed Russian online operations in 2014 and 2015.

The relationship is complicated by the suspicion that the Trump campaign worked closely with the Russians. This makes the matter highly political, which is clearly expressed in congress and reflected in the press. Special Counsel Mueller is assigned to the case with broad authority. In anticipation of his conclusion, the matter is marked by leaks and speculation. In 2017, the New York Times reported that the investigation had discovered contact between Russian intelligence and members of Trump's campaign staff. Several people have been convicted for lying to the FBI. So far, it remains unclear what Trump's contacts assisted with, whether this was exclusively a mix of different roles, or if relationships were established that brought Trump into a dependency on Putin. Certain of Trump's behaviours have contributed to these speculations.

In January 2017, a classified report was leaked to the press. Christopher Steele, a British former intelligence officer and Russia expert, claimed that Moscow holds compromising information on Trump, including footage of him with prostitutes at a Moscow hotel in 2013. The report was financed by the Clinton campaign and the Democratic Party.

A great deal of excitement and anticipation is placed on Special Counsel Mueller's report, concerning whether it will provide a basis for federal charges against the president. However, we can already draw some conclusions. The Russians attempted to influence the outcome of the election and the result ended up being what they desired. The case has weakened the mandate of the president and has produced a suspicion that Trump has a hidden agenda. It has likely been relatively easy to access the Democrats' servers, as the password was leaked. Influence through social media is far more interesting. This is a key point in Mueller's investigation. The company Cambridge Analytica is central here. It was founded in 2013, and Breitbart editor and Trump collaborator Steve Bannon was the vice president of the company for a time. The business concept is to gather information on voters in order to map their attitudes and preferences. This makes it possible to customise a political message to give it the greatest possible impact.

Cambridge Analytica

Dr. Michal Kosinski is a professor of psychology at Stanford University, USA. In the period from 2008 to 2014, he studied at Cambridge University, where he developed a method for determining people's important characteristics on the basis of "likes" given on Facebook. This is an interesting and potentially frightening application of what we call machine learning through the use of large volumes of data. Alongside his colleagues, he made a Facebook app and invited users to fill out a questionnaire that would be used to determine the personality traits of the respondent.

This was a standard test. Three million people agreed and gave their information. This led to three million profiles that were used in research. He then developed algorithms that, on the basis of a person's provided “likes”, would determine the same personality traits. The results were baffling. Based on a relatively low number of “likes”, he could with great accuracy estimate the same personality traits that were discovered through traditional analysis of the questionnaires. More “likes” gave a clearer answer. The machine proved to be able to compile and interpret the information located in seemingly unstructured declarations of sympathy (likes) far better than a person could. There were business opportunities here.

Kosinski proceeded and tested whether the method could be used for effective marketing in which customers receive advertisement customised to their personality. He conducted multiple advertising campaigns on Facebook, one of which involved cosmetics. The advertisements were designed in two ways, one to have an impact with introverts and one to have an impact with extroverts. The advertisement was sent to 3 million people. It worked. The recipients were 50% more open to purchasing the cosmetics when they were targeted at their personality type.

In 2014, the firm Cambridge Analytica signed an agreement with Aleksandr Kogan, one of Kosinski's colleagues at Cambridge University. 270,000 Americans responded to a new survey of personality traits and political preferences in return for a financial compensation of 2-5$. The respondent was required to have previously voted, and that she/he had to log in using their Facebook account, which Kogan thus also gained access to. Cambridge Analytica paid for it. By collecting data, including data on the respondents’ friends, Cambridge Analytica acquired information on many millions of voters. Facebook claims the contract only allowed them to collect information on those who had consented and been paid. Kogan contests this.

Everything was in place to operate a personally targeted election campaign for Donald Trump. Cambridge Analytica has assisted in a number of elections in multiple countries. It is well known that Senator Ted Cruz used the company, but terminated the contract after the expected progress did not materialise. This indicates that Kosinski's method is not a miracle technique that always brings success. Only when other conditions are met does it give results.
Although the method first and foremost has been discussed as people seek an explanation for Trump’s surprising electoral victory, it may be used for many other purposes than influencing voters. It has proved to be effective for determining sexual orientation, ethnicity, intelligence, trauma, political stances and predisposition to drug addiction on the basis of "likes” alone. This is cause for concern. It is still an unanswered question whether information Cambridge Analytica was used for Russian online operations, but it cannot be ruled out.

The 2017 French presidential election.
The results of the US presidential election and the Brexit referendum in the United Kingdom came very unexpectedly and caused unease in influential communities. Explanations were sought, and a justified suspicion was raised that Russia had played a covert role, particularly in the USA. NSA chief Mike Rodgers warned about Russian involvement in the upcoming French presidential election.

After the crises in Ukraine, it was clear that Russia wished to weaken NATO and the EU and to bring an end to the economic sanctions on the country.

7. Hybrid measures

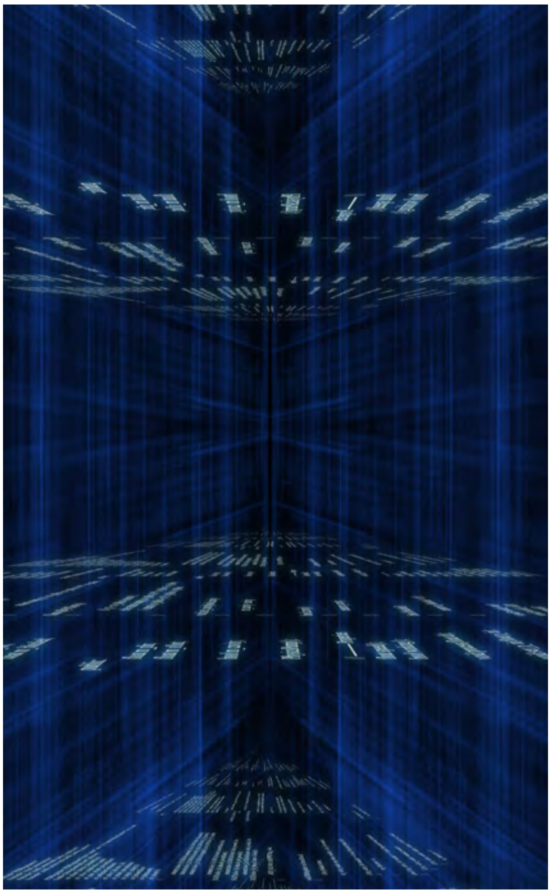
The leader of National Front, Marie le Pen, was strongly critical of French immigration policies, NATO and the EU. The Russian websites RT and Sputnik consistently presented her positively in the election cycle. The president who was later elected, Emmanuel Macron, described them as propaganda agents for National Front. In a meeting with President Putin, le Pen stated that she supported Russia's annexation of the Crimea and would eliminate the economic sanctions. She was clearly Putin's favourite in the presidential election. After French banks refused National Front loans on the basis of their racist stances, they received Russian loans for their campaign in 2014. There was significant concern that Russia would try to influence the election. This was speculated in several types of incidents.

Two days before the first round of voting, tens of thousands of e-mails from Macron's campaign organisation were leaked. The e-mails were shared on social media by WikiLeaks and by many American activists. The leaks received immense media attention, but Macron was able to endure it well. Firstly, the e-mails did not reveal any particularly censurable conditions, on the contrary. They confirmed the impression that Macron had been above board throughout the campaign. Although certain e-mails contained compromising contents, these were clearly falsified and had been done so in a highly amateur fashion.

The election results indicate that the leak had a minor impact, Emmanuel Macron won the second round with twice as many votes as Marie le Pen. The big question now is who was behind the e-mail hacking.

Flashpoint, an American cyber-security company, concluded with "moderate confidence" that Fancy Bear, a hacking group with ties to Russian military intelligence, was behind the hacking. Guillame Poupard, chief of French cyber-security, stated to the Associated Press that the hacking was so generic and simple that nearly anyone could have done it. The image was therefore somewhat unclear.

It was clear that Russia supported le Pen, and she signalled support to Russia in key issues. Russia therefore had strong motives to get her elected. Even so, the leak of the e-mails was amateur and in contrast with the image of skilled Russian hackers. No mapping of major French voter groups had been conducted in the manner the technology behind Cambridge Analytica opened for. The most effective tool for influencing may not have been available, but the situation may be different in future elections. Or perhaps le Pen's situation was so hopeless that Putin would not show his cards.



Conclusion

It is important that national readiness takes hybrid threats seriously. Changes to society and technological development make life better for large groups of people, but they also create vulnerabilities that can be exploited in a world rife with conflict. The peace optimism of the '90s has been replaced by a range of new and unclear lines of conflict. Russia has shown the will and the ability to use means forbidden by international law to secure its interests and has continued its heritage from the Soviet Union of investing in technology and natural sciences for political and military purposes. At the same time, the economy does not allow for defence investments on the level of the USA or China. They have to be creative, and they must be politically and technologically smarter than their opponents. Therefore, it is important that we not only concentrate on known threats, but also systematically search for new threats before we are exposed to them.

It is clear that cyber-crime is here to stay, from the most trivial to the more advanced. Public and private businesses will have to spend considerable resources on robust technological solutions, training and organisation to protect their assets. This is understood among the responsible parties and will be done. However, when it comes to severe hybrid threats against the country's sovereignty and security, we stand before resource-rich and creative agents. Creative means will likely not be revealed before it is critical, and by then it will be too late to learn. The Hybrid Study reveals a need for information, instruction and guidelines. It is important and appropriate that the new Security Act enables security authorities to forge a better understanding of what may strike in terms of sabotage, espionage and terrorism.

If Special Counsel Mueller gets to the bottom of all the suspicious conditions surrounding the US presidential election, the surprising election results may be held up as the most successful hybrid operation ever. The e-mail leaks targeting Macron in the French presidential election had a minor impact, however, but there are several conditions that distinguish the two matters. One important difference is the content of the e-mails that were leaked. Another was that Cambridge Analytica had mapped the attitudes and preferences of millions of voters in the USA, particularly in swing states. This made it possible to individually customise the political platform, both online and in the presidential candidate's speeches. Trump succeeded at this, but Cruz failed.

What should we learn from this? Fundamentally, Cambridge Analytica builds on the fields of mathematics, machine learning, big data, psychology and marketing. The research community at Cambridge University showed that a machine can, with far greater precision than a human, determine a voter's personality, including preferences and antipathies, on the basis of scattered and seemingly random information. This will of course be developed further for marketing legal products, but in the USA, there is still investigation concerning a possible complicated cooperation between a foreign power and an election campaign organisation. This places requirements on traditional cyber-security efforts to prevent confidential information from going astray, but it is not enough. When fake news is spread to weaken a state, it is important that official information is believed and that the authorities have trust as we experienced it on 22 July 2011. Therefore, we have a common interest and responsibility in further developing the Norwegian society of trust, so that we also trust the politicians we did not vote for.

7. Hybrid measures

7.1 Hybrid threats, what now?

Richard Utne, the Norwegian Armed Forces

"The international consensus on 'hybrid warfare' is clear: no one understands it, but everyone, including NATO and the European Union, agrees it is a problem".

- Multinational Capability Development Campaign (MCDC) Countering Hybrid Warfare (CHW): Understanding Hybrid Warfare (2017).

In 2017, a Norwegian-led multi-national capacity and development project presented the report Understanding Hybrid Warfare. The report claims that to solve a problem, one must first understand it, and points out that there is no overall consistent definition of the term hybrid threat. Starting out, it is therefore important to establish a thorough approach to the term. Hybrid threats are represented by a broad spectrum of military, political, financial, civilian and information instruments that are targeted at civilian society and the private sector. What seem to be small attacks in isolation may turn out to be synchronised attacks in which the use of the entire spectrum of hybrid threats in total produce an effect that far exceeds that of a conventional military attack. Research points to such low-intensity conflict being the most likely form of future warfare on the western hemisphere, where the battle will overwhelmingly be linked to the narrative. The signature of hybrid threats is that they are designed to create an effect, while still remaining below the alert level of existing defence mechanisms. With a high degree of believability, they thus cannot be linked to a single agent, which also makes it difficult to reach a consensus for collective reaction.

An agent targeting hybrid threats at Norwegian interests may be imagined to have long-term political strategies that go far beyond our own political time frames. Thus, our perception of the norm may shift gradually, until we eventually establish a perception of a new normal state. International social networks with investments in critical infrastructure are perceived as natural in our globalised world. This is relevant to the business community, for total defence and for NATO, as resources and critical infrastructure that are important components for civil society as well as for total defence are owned by the private sector to a greater degree. On average, more than 50 percent of satellite communication used for defence purposes is from the private sector, and about 75 percent of host nation support for NATO operations and exercises is collected from commercial infrastructure and services.

The relationship between typical operators in the business community is mutually independent of the various support functions, providers and supply segments being adequately robust to withstand a hybrid attack, whether it involves politics, finances or reputation. Article 3 of the Atlantic Treaty describes civilian readiness and resilience as fundamental conditions for individual and collective defence. Precisely because hybrid threats target the civilian and private sectors, the costs linked to robustness and resilience are a responsibility that rests upon the business community instead of military readiness in the traditional sense.

Because civilian and military readiness, as well as crisis management are mutually dependent on each other, the government's strategy for total defence ("Support and cooperation 2018") explains that continuous cooperation is required to utilise society's collected resources as best as possible, thus allowing for a good social economy.

Responsibility, closeness, equality and cooperation are national principles for cooperation in readiness and crisis management. However, as there is a lack of adequate sensors in the business community that can identify (potential) hybrid threats, responsibility, closeness and equality risk preventing reports to a (hitherto non-existent) overall body that can compile incidents across the entire spectrum of means to identify and if possible, issue an early warning concerning an ongoing synchronised hybrid attack. One of our biggest challenges related to hybrid threats today is therefore not a lack of ability to cooperate or barriers and counter-measures, but that cooperation, barriers and counter-measures are reactive instead of being proactive. Therefore, the Hybrid Study of the Norwegian Business and Industry Security Council is an important contribution to responsible authorities investing proactive measures in the business community for support and cooperation. This is a good social economy and a step on the way to 2%.

Richard Utne has long and varied experienced in risk management and security leadership in both the private and public sectors. In 2018, Utne was the project manager of NATO’s civilian committee Transport Group Ocean Shipping: Kinetic and Hybrid Threats to the Maritime Community in the North Atlantic Ocean and the North Sea. This article exclusively represents Utne's own views.

7. Hybrid measures

7.2 Norges Bank and hybrid threats

Carl-Axel Hagen, Director of Security, Norges Bank

With a global threat profile marked by intelligence, organised crime and terrorism, Norges Bank shall complete its tasks with a high degree of security for its personnel, its functions and its systems. Norges Bank manages a number of critical functions, including the payment system, the treasury, financial crisis management and the government's foreign pension fund.

These days, there has been a change in how conflicts play out. A preference has developed for the use of hybrid measures that increasingly also affect civilian institutions. At the same time, the geo-political landscape is in flux in a manner that may lead Norges Bank, being Norway's central bank, to involuntarily be perceived as a political and diplomatic agent. In Ukraine, cyber-attacks including espionage and sabotage have been observed, also targeting the financial sector. In other countries, there have been influencing operations targeting central bank management in what are likely attempts to weaken the reputation of the finance sector.

Hybrid threats seek to reduce the political space of action by using different means of power against vulnerabilities and cracks in society. The authorities that hold the total overview are the ones that can best determine whether Norway is exposed to hybrid threats.

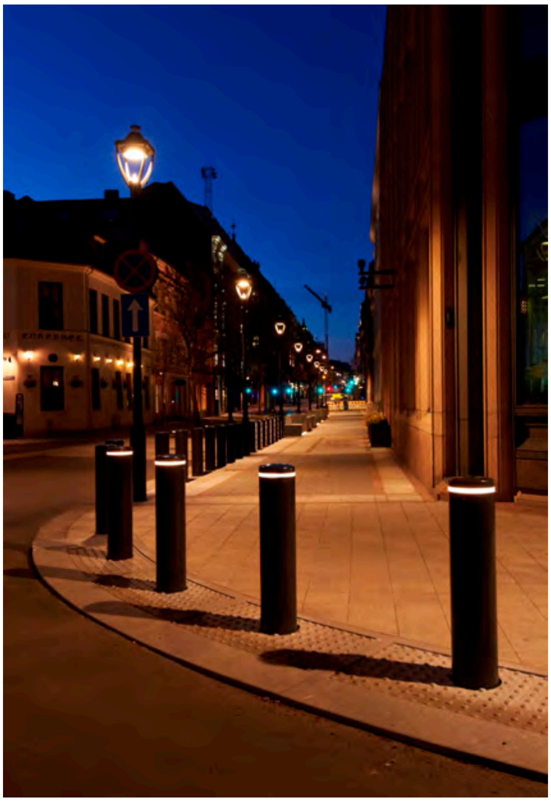
Norges Bank supports the authorities in this task through four concrete measures. First of all, the bank has an intelligence community that continuously monitors the global threat profile and identifies incidents that may affect Norges Bank.

Secondly, there is close cooperation between the bank's physical- and cyber-security communities. This means that Norges Bank is able to see the connection in intended undesired incidents that take place in physical and logical domains.

Thirdly, the security community of the bank has conducted active and targeted dissemination of knowledge concerning hybrid threats to top management and system owners of Norges Bank's assets, so that they have an understanding of how security incidents linked to the bank's objects, infrastructure and information systems may have political consequences.

Finally, the bank has maintained close dialogue with the authorities and regularly reports on relevant security incidents that affect Norges Bank.

Through these four measures, Norges Bank is able to assess the degree to which intended undesired incidents may be used to affect political freedom and to report to relevant authorities.



Five recommendations for the business community

Include security-related themes in regular conversations with employees, as topics in projects and in daily operations. Through regular conversations and raising awareness, one can establish a culture with space to discuss security-related challenges and incidents. This provides the business with an opportunity to implement security measures proactively.

Regular reminders concerning measures and using management systems effectively to determine whether the measures serve the purposes. Through regular assessment and follow-up of implemented measures, the business will keep an updated image of its own security consciousness and security efforts.

Asset and vulnerability awareness – are a foundation of good company culture. Hybrid threats do not necessarily target those who have the most money in the bank. Social networks, geographical placement or company competency are conditions that should be considered to assess the business's assets and vulnerabilities.

Threat awareness – just as companies have good knowledge of their market, they should remain updated on the trends, agents and incidents that comprise the threat profile. PST, the Intelligence Service, DSB and NSM annually publish different threat assessments with free information on which threats your business may face.

Global trends – by familiarising oneself with global trends, one can to a greater degree understand the threat profile hybrid threats represent. It is important to understand that one is a piece in a greater game.

Considerations

For 2019, the government allocated 25 million NOK to PST for work with hybrid threats and cyber-threats. Thus, PST receives personnel and technology that provides an improved capacity in the digital space to reveal, prevent, handle and investigate the most severe attempts at espionage, sabotage, influencing operations and compound (hybrid) threats. The allocation will among other things provide a foundation for further development of PST's cooperation with the Intelligence Service, NSM and KRIPOS. NSR believes this is a positive investment.

Further investment in total defence may contribute to strengthening the robustness of society with regard to hybrid threats. The total defence concept revolves around there being mutual support and cooperation between the Norwegian Armed Forces and civilian society across the entire spectrum of crisis, from peace, via security policy crisis to war. This requires the business community and the authorities to maintain close dialogue and to share information.

Hybrid threats and the threat profile we see today does not take public sector divisions and areas of responsibility into account. The situation we now face therefore requires proactiveness, coordination across sectors, departments and areas of responsibility, as well as an anchored and shared situational awareness. By experience, ordinary crisis management focuses more on the reactive. Therefore, private, civilian, police and military sectors must provide for a more mutual flow of information and exercises related to proactiveness.

8. Measures

- We will here present strong advice for the business community as well as an overview of hybrid threats and preventive measures.

8. Measures

Method	Purpose
Information influencing	
Influencing school curricula	Developing a positive attitude to certain agents and/or sowing division between groups in society (language, religion, history).
Influencing elections	Weakening trust in democratic election results, promoting specific candidates, creating division and weakening decision processes.
Fake news	Sowing division, creating a "reality" that harms the reputation of cities and states, weakening decision processes, sowing distrust.
Organisations financed in foreign countries	Retrieving and collecting information, maintaining a network of influencers, psychological influence, identifying weaknesses.
Media financed in foreign countries	Media financed in foreign countries. Information influencing, counter-acting integration.
Cyber-influencing	
Attacking/disrupting public administration information systems	Sowing distrust and insecurity, making room to promote their own views, financial benefits.
Breaching government databases and leaking information	Collecting information, sowing distrust and insecurity, financial benefits.
Weakening/disrupting critical infrastructure **Through cyber-attacks**	Sowing distrust, insecurity and testing abilities.
Overloading public services	Creating disorder, distracting attention.

The table is collected from and reproduced with permission from the Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats report "Helsinki in the era of hybrid threats – Hybrid influencing and the city" (23.08.18).

Example	Preventive measure
Attempts to weaken the position of the Swedish language in Finnish schools.	Awareness of the phenomenon. Creative educational solutions in cultural subjects.
Financing of specific candidates Hacking of electronic election systems.	A protected physical election system. Openness in campaign financing.
Exploiting real or fake incidents by linking a criminal action to a specific group of people or terrorism.	Improving media knowledge in education. Equal and even communication flow that does not leave a vacuum for false information. The will and ability to address difficult and politically sensitive topics in communication. Openness.
Supporting or operating a seemingly ideological organisation and using it to exploit the role and "voice" of a group of people. Exploiting associations to spread information.	Supporting the activities of trustworthy organisations. Representing different groups of people in decision processes and public discourse.
Foreign-language radio channels and digital media. Political exploitation of the position of journalists.	Media produced by minorities themselves and support for these. Expansive foreign-language communication from public administration.
Disruptions to the government's payment of salaries through information systems.	Systematic information security Response plans.
Hacking of patient data in healthcare and social work institutions and employee extortion.	Systematic information security. Response plans. Maintaining secure routines for procurement and tendering.
Sowing distrust, insecurity and testing abilities. Disruptions of critical operations, such as the power supply in cities.	Cooperation with key organisations. Improving readiness in homes and raising awareness.
Disrupting and overloading case handlers.	Technical preparations to handle major progress. Preparing for communication in extreme situations.

8. Measures

Method	Purpose
Physical influencing	
Object recognition	Retrieving and collecting information, showing force, identifying vulnerabilities, testing the opponent's capacity for detection.
Drones	Retrieving and collecting information, physical attacks, creating a frightening atmosphere, division.
Protests	Creating disorder, distracting attention., polarisation, weakening the sense of security.
Exploitation of vulnerable individuals	Retrieving and collecting information, acquiring authority and entry options, radicalisation.
Financial influencing	
Property purchases	Damage/disrupt/map infrastructure, apply political pressure, show presence.
Company ownership	Map, retrieve and collect information.
Supply chain infiltration	Retrieve and collect information, as well as imped-ing, Disrupting or destroying deliveries.
Corruption	Create a negative impression, extortion, sow discontent, influence decisions.

Example	Preventive measure
Infiltrate secure facilities with fake access permission.	Raise awareness of the risk. Control and monitoring of access rights.
Flying drones in public areas to disrupt and distract authorities.	Forbidden areas for drones. Clear legislation on this point for the police’s ability to enforce. Taking drones into consideration for urban planning.
Supporting and reinforcing protests from extremist organisations, as well as supporting organisations on the opposite side to increase unrest.	Prevent social exclusion. Close cooperation and presence between the police and the city/municipality.
Contributing to the radicalisation of socially excluded persons, extortion of individuals in critical positions.	Prevent social exclusion. Background checks and management of person-related risks.
Purchases of properties near critical infrastructure or critical operations, such as water management facilities or power stations.	Identify critical operations and supply chains.
The purchase of technology companies for access to customer info or marketing access.	Restrictive legislation.
Gaining access to critical information through a supplier.	Identifying critical operations and supply chains. Critical assessments of procurements and outsourcing.
Bribing decision makers or elected persons and/or exposing them to sow distrust.	Openness. Processes for risk management and assigning responsibilities for internal audits.

www.nsr-org.no

Næringslivets sikkerhetsråd

Against crime - for business and society