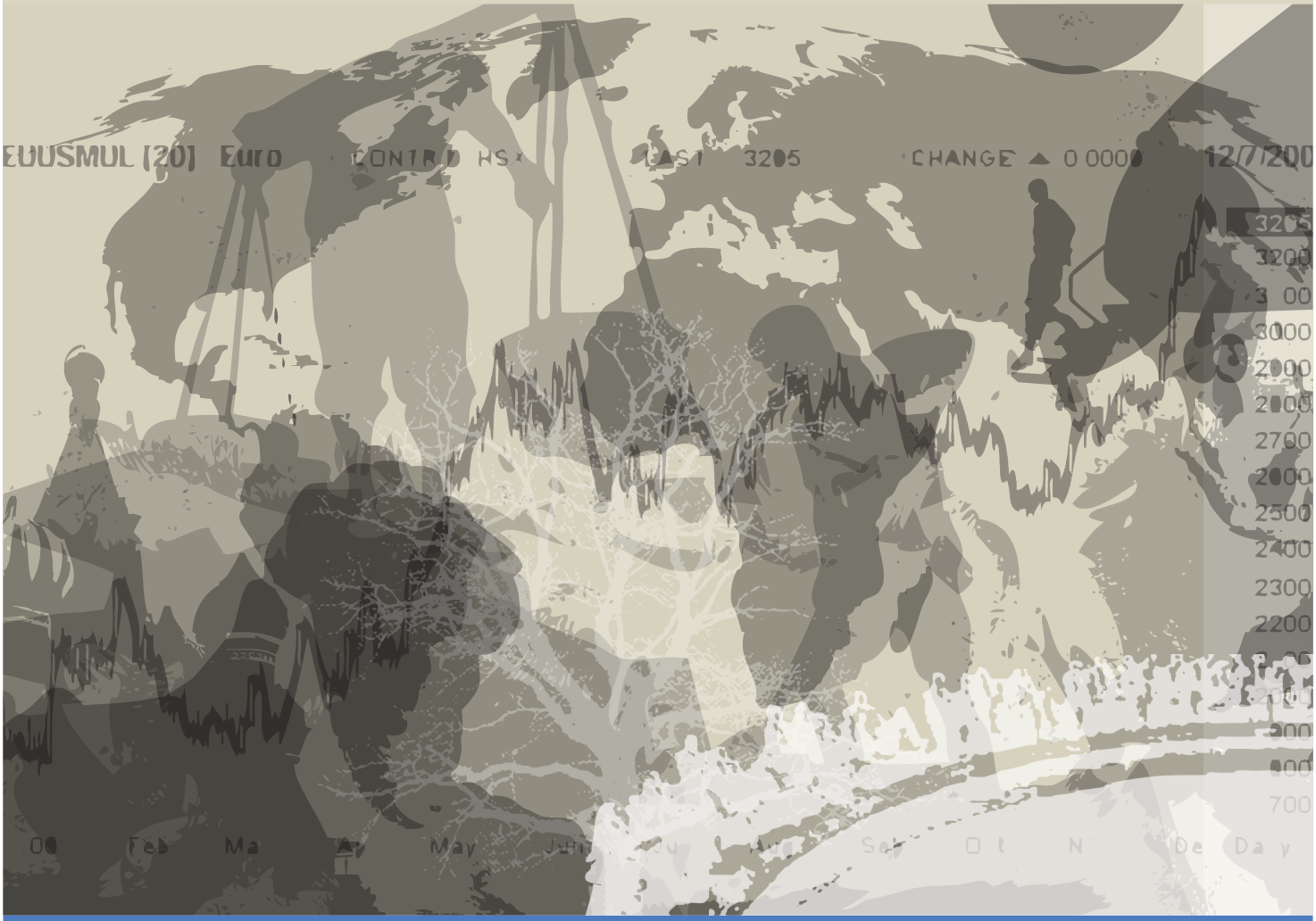
Norwegian Institute of International Affairs

Cyber-weapons in International Politics

Possible sabotage against the Norwegian petroleum sector

Lilly Pijnenburg Muller, Lars Gjesvik and Karsten Friis



NUPI Report
3 / 2018

Publisher: Norwegian Institute of International Affairs

ISSN: 1894-650X

Visiting address: C.J. Hambros plass 2d
Address: P.O. Box 8159 Dep.
NO-0033 Oslo, Norway
Internet: www.nupi.no
E-mail: info@nupi.no
Fax: [+ 47] 22 99 40 50
Tel: [+ 47] 22 99 40 00

Cyber-weapons in International Politics

Possible sabotage against the Norwegian petroleum sector

Lilly Pijnenburg Muller, Lars Gjesvik and Karsten Friis

Published by the Norwegian Institute of International Affairs

Contents

Foreword: Background and acknowledgments

The use of digital weapons is a rising global problem. Society is rapidly becoming more digitalized – and thereby more vulnerable to attacks. These vulnerabilities are increasingly abused by states and other international actors: Information is stolen, and sabotage occurs.

Politically motivated digital attacks against petroleum-sector infrastructure represent one such threat, but this has not attracted as much attention by politicians and business leaders as other security challenges in the sector.

In an international crisis, Norwegian oil and gas deliveries to Europe could be attacked on a scale far exceeding what the private and public sectors experience on a daily basis. Such attacks could be aimed at stopping or hindering the physical delivery of petroleum, with direct economic, security and political implications beyond the digital domain.

With the digitalization of the physical infrastructure, and the increasing trend among states to develop the capacity to perform offensive cyber operations (Bildt 2017), the threat seems set to increase in the years to come. Digital sabotage against critical national infrastructure (CNI) has been rare, but is growing in scope and magnitude in connection with international crises and conflict (PST 2017, 2018; NIS 2017).[1] A cyber-attack seldom occurs in isolation, and it often takes place within a geo-political context. An evaluation of the risk of cyber-attacks on Norway's petroleum sector must therefore take its point of departure in the broader geo-political security picture.

[1] As we will return to below, the Norwegian Petroleum industry is legally not defined as part of the Norwegian CNI at the time of writing. However, when the new Security Act is enacted, certain parts of the sector may be defined as 'skjermingsverdig infrastruktur' or as 'grunnleggende nasjonale funksjoner' ('basic national functions'). See also footnote 20.

According to the Norwegian Police Security Service (PST) and the Norwegian Intelligence Service (NIS), China and Russia are the countries that carry out most cyber-attacks against Norwegian digital systems. These attacks are used primarily to gather information about political decisions, defence installations and industrial technologies (PST 2017; NIS 2017). However, intelligence operations in the digital domain, and particularly those aimed at CNI, may also serve as preparations for sabotage in the event of a political crisis or war.

The political tension that has developed between Russia and the West since the Russian annexation of Crimea in 2014, has put a new focus on the concept of 'hybrid warfare', where non-military power is used systematically side by side with military means to obtain political goals. While few today believe that Russia and NATO will end up in conventional warfare, a tense political situation may lead to Russia using new tools of power, among these targeted digital attacks against CNI (Cullen and Reichborn-Kjennerud 2016). Such attacks could lead to a destabilized situation, and decrease trust in state and private sector actors. Norway, like other countries, needs to have a holistic view of the security threat, and not limit itself to focusing solely on conventional military threats.

Norway delivers approximately 30% of the gas and 10% of the oil imported by the EU, and 30–40% of the gas imported by the UK, Germany and France.[2] If the political situation between the West and Russia deteriorates further, we cannot rule out the possibility that Russia may use untraditional tools, such as digital attacks, to affect deliveries from other competing suppliers to the energy market in Europe. This is a worst-case scenario, but could have severe consequences for the Norwegian petroleum industry and the Norwegian standing as a stable and predictable energy producer in Europe.

In 2014, the oil sector in Norway experienced a large-scale cyber-attack: More than 50 Norwegian oil and energy companies were attacked, with Statoil as the main target (Munson 2014). The

[2] For information on the EU and its supplier countries from the webpages of the European Commission, see for instance: https://ec.europa.eu/energy/en/topics/imports-and-secure-supplies/supplier-countries

Norwegian National Security Authority (NSM) issued a statement that the hackers had done research beforehand and gone after key functions and key personnel in the various companies. The attacker's goal was to install a keylogger, which would allow passwords to be stolen, with the ultimate aim of siphoning intellectual property out of the target organisation. The attack uncovered shortcomings in terms of communication channels and response mechanisms between the private and public sector in Norway (NOU 2015:13).

The NOU (2015:13) 'Digital vulnerabilities – a secure society' argues that there are indications that the value chain in the petroleum sector is a possible target for digital attacks, with production platforms, refineries, pipelines, and shipping terminals cited as the most critical sites. The report also points out that the industry is international and consists of Norwegian as well as foreign companies. As both the industry and the threat are international, the solution must be too.

The vulnerability of the Norwegian petroleum sector must be seen in an international context. Threats, actors and response environments all operate within in a holistic threat picture and need to be considered within the relevant political climate.

Further, the location of the current cyber-threats within the larger strategic context, and the role of the public and private sector in addressing such threats, is assessed. The report highlights some of the key challenges found in handling such threats today, in order to assist actors in the public and private sectors in recognizing where the main challenges lie.

The issues are complex. In this report, we have tried to address and balance the views and interests of a diverse group of stakeholders from the Norwegian government, as well as elements of the private sector (notably the petroleum and the technology sectors). Without attempting to propose a path that can reconcile all conflicting interests of these stakeholders, some key issues and challenges in bringing them closer together are highlighted, with the aim to align interests to move towards productive solutions to shared challenges, in the interest of all.

The research was made possible by the financial support by the Ministry of Justice and Public Security, Ministry of Defence, Ministry of

Foreign Affairs, Petroleum Safety Authority (PSA), Norwegian Oil and Gas, Statoil and Gassco. In addition, NUPI wishes to thank NSM/NorCERT, PST, NIS, NKOM, Simula and SINTEF – organizations and individuals – who participated at seminars and interviews, in panel discussions, research and drafting that have helped to shape the ideas presented in this report. While all contributed, the report does not represent a consensus viewpoint of all parties involved in the task force process.

Executive summary

In recent decades, the petroleum sector has embraced the growth of digital solutions, moving its business activities and operations into an information technology environment. This transition has provided great benefits for the sector – enabling efficiencies, lowering costs, establishing new products and markets, enhancing internal cooperation, and helping companies to utilize and trade petroleum internationally. But as the technology has developed, new risks have accompanied these benefits: The petroleum sector is increasingly vulnerable to theft of intellectual company information and the disruption of business operations through digital means. These risks have grown due to recent international cyberspace activities of hostile states and non-state actors, who have attacked private-sector entities, motivated by political as well as financial objectives.

This report examines the challenges in securing the petroleum sector in a digital age within a geo-political context. We will argue that the cyber security measures taken by the public and private actors in the petroleum sector are not commensurate with the nature of the cyber-threat today. The report will address these shortcomings.

Political discussions concerning the digital security of the petroleum sector in Norway have been limited. To the extent that discussions are held, there are two camps: Those arguing that the state is doing too little, and those arguing that state regulations are too costly and burdensome. What has been missing is a more nuanced discussion of the topic, and an understanding of the international dimensions of the field. What measures should be the responsibility of the private sector? Where does the state come in, before a fully-fledged national attack unfolds? An attack can take months, even years to be discovered – when and where do the authorities engage? What is the role of the government in developing frameworks, laws, and regulation, and a set of norms to such action? How should policy and law be updated to support the private sector in ways consistent with the values and interests of both sides, and capable of evolving as new technologies are developed?

The initial section of the report provides a geopolitical background and context to the discussion. Starting with the Norwegian energy sector and its dependencies, before discussing Norway, Russia and their energy relations. Secondly, the various cyber-organizations within Russia and their possible connection to the Kremlin are examined, and the importance this has for understanding where a possible cyber-threat may come from is assessed. Certain other states and organizations that may pose a threat are also briefly discussed.

The next section focuses on digital threats, using three illustrative cases: the cyber-attacks on the Ukraine electricity grid in 2014–2016, and the NotPetya attack of 2017, to illustrate the cyber security challenges in the energy sector.

The report then turns to specific vulnerabilities and digital vulnerabilities in the Norwegian petroleum sector. The discussion is divided into *prevention* and *response*, to clarify the distinct mechanisms for dealing with challenges at various stages. The report particularly points to challenges related to supervision, information flow, supply chains and security standards, exercises, as well as various topics related to roles and responsibilities.

By identifying and highlighting these challenges, the report seeks to help in making the petroleum sector better capable of defending its most valuable assets and data from digital sabotage. Both the private and the public sector have responsibilities in this regard, but there are grey-zones, ambiguities and uncertainties that need to be addressed. The financial and political consequences of a successful attack could be significant and serious, thus warranting a thorough discussion and due process to address shortcomings.

1. Political Context: Geopolitics and energy export

The petroleum sector holds a key position in the national economy in Norway. In 2014, it accounted for 20% of Norway's GDP, 27% of the state's income and 46% of all exports (Olsen 2015). Thus, the security of the petroleum sector has obvious ramifications beyond the various companies who own the vital infrastructure – the sector is crucial for Norway as a nation. While the government is involved in most aspects of securing the petroleum sector – from health and safety to military training for possible terror attacks – the complexity of securing against cyber threats represents a constantly evolving challenge.

Norway exports 97% of all the gas it produces, making it the world's second largest gas exporter. Most of Norway's export of crude oil goes to the European Union, and almost all its gas goes through pipelines to the EU (Norsk Petroleum 2017). In Germany, the UK, Belgium and France, Norwegian gas accounts for between 20% and 40% of total consumption (ibid.). Norway is dependent on its exports to the EU in an economic sense, with the EU as its largest trading partner. As for the EU, it relies on a few countries – Norway among them – to cover its energy needs. The 2014 EU Energy Security Strategy identifies this dependence on 'particular suppliers' as a significant risk to its energy security, and recommends a reinforced partnership with Norway, *inter alia,* as one solution (European Commission 2014). However, the European gas and energy market is evolving, with diversification in new suppliers and sources, such as Liquefied Natural Gas (LNG). The growing use of renewables is also likely to impact the petroleum market over time. As a greater share of the petroleum trade takes place in the spot market, European customers may be less dependent upon fixed supply than before, as alternative suppliers can be found after some time.

Russia is the largest oil and gas supplier to Europe. Although Norway has increased exports in recent years and Russia has seen its exports fall in the wake of the annexation of Crimea, Russia still

provides the largest share of both fossil fuels (Eurostat 2017). According to figures from the EU, the share of Russian gas in the EU has dropped by 40% in recent years, down from its peak in 2010 (ibid.). Moreover, tensions between Russia and the West have grown as the crisis in Ukraine has unfolded, resulting in sanctions and countermeasures (Haukkala 2015). In addition, the US Congress in 2017 emplaced sanctions in the wake of the Russian involvement in the US presidential elections. The effects of these sanctions have made themselves felt in Russia, and could affect the trade in energy, and what kind of business energy companies can do with Russia (Nougayrede 2017). With gas trade increasing globally in the wake of developments in LNG, Russia has used unconventional means, such as media campaigns, to discredit alternative sources of gas (Atlantic Council 2017).

For Russia, the use of gas delivery as a political tool is nothing new. The overlap between political and economic considerations is clear: Energy is used to achieve political goals, and political moves are made to promote energy (economic) considerations. The petroleum industry and the state are interwoven, with considerations and actions at times overlapping and supporting each other (Orttung and Øverland 2011). Following its annexation of Crimea, Russia has used direct cyber-attacks on the energy sector as a political tool, as detailed later in this report.

With tensions growing between Russia and the West, relations between Norway and Russia have become strained. A low point came in February 2017, when the Russian ambassador to Norway sent a 1400-word letter to the Norwegian media condemning Norway's attitudes to Russia (*Verdens Gang* 2017b). This occurred in the wake of PST singling out Russia as a threat to Norwegian interests in their yearly threat analysis report (PST 2017). Only a few months earlier, Norwegian MPs Bård Vegar Solhjell and Trine Skei Grande had been denied visas for an official visit to Russia, after being placed on a list of *persona non grata*. Russia framed these incidents as a response to Norway's adherence to the sanctions that had been imposed following the annexation of Crimea in 2014 (*Verdens Gang* 2017b).

In the digital domain, this has arguably also started to manifest itself: in February 2017, PST alerted the media that they suspected

themselves, the Labour Party, the Ministry of Foreign Affairs and the Army to have been hacked by a Russian Advanced Persistent Threat (APT), APT29 (*Verdens Gang* 2017a). Similarly, the UK has reported being hit by Russia, with the media, elections and energy sector targeted in 2017. Energy relations between Norway, the EU and Russia have also been a subject of controversy – notably when, in a meeting with the international press regarding opportunities for Russia/EU cooperation, Vladimir Putin declared that Norwegian energy resources were 'depleting', and urged Germany to look to Russia to supply its energy needs *(Dagens Næringsliv* 2017). In sum, the tensions between Russia, the West and Norway has led to incidents, both in and outside cyberspace.

A cyber-threat from Russia?

According to the Norwegian Intelligence Service (NIS), actors linked with Russia have infiltrated infrastructure in the West (Lunde 2017). In February 2015 the US Director of National Intelligence, James Clapper, had informed the US Congress that: 'the Russian cyber threat is more severe than we had previously assessed' (*The Diplomat* 2015). More recently, Admiral Michael Rogers, who leads the NSA and US Cyber Command, stated: 'Russia has very capable cyber operators who can and do work with speed, precision and stealth' (Rogers 2016). Yet, he also noted, while Russia's mapping of vulnerabilities is extensive, this has not yet led to coordinated attacks or attempts causing physical destruction beyond Russia's 'near abroad'. In any case, Russia, the government and its assorted connections with occasionally government-sponsored cyber-hackers and group members have integrated cyber-operations into Kremlin military doctrine, using cyber-tools against foreign as well as domestic adversaries (Connell and Vogler 2017). There is no doubt about Russia's cyber capability, yet to grasp how, if and when Russia might use cyber-threats in a political situation, we need to understand the construction of the Russian military and how (information) warfare is perceived.

Russia holds advanced cyber-capabilities, and in recent years Moscow has increasingly demonstrated its readiness to use offensive cyber-operations in situations other than war in order to deter adversaries and/or affect political and economic outcomes in neighbouring states (BBC 2017b; Connell and Vogler 2017). Russia and the West view cyber-operations differently – from how cyber-

warfare is perceived, to how cyber-capabilities are employed and how cyber-operations are viewed within the information warfare landscape.

Russian military theorists do not generally use the term 'cyberwarfare': cyber-operations are understood within the broader framework of *information warfare*. 'Information confrontation' or 'information war' is understood as a broader and inclusive concept covering a wide range of activities. It applies to hostile activities that use information as a tool, or a target, or a domain of operation, and includes both computer and human information processing, in effect the cognitive domain (Giles 2016). Russia does not see information warfare as an activity limited to wartime: 'it is not even limited to the initial phase of conflict before hostilities begin, which includes information preparation of the battle space' (Antonovich 2011). Instead, it is seen as an ongoing activity regardless of the state of relations with the opponent, and may include computer network operations alongside psychological operations, strategic communications, influence, electronic warfare, information operations, computer network operations and electronic warfare (Giles, 2016; Connell and Vogler 2017). For example, in connection with the 2017 British general elections, Ciaran Martin, chief executive of GCHQ's National Cyber Security Centre (NCSC), stated that Russia sought to undermine the international system and accused Russia of having attacked Britain's media, telecommunications and energy sectors (BBC 2017a). And yet, there was no direct conflict between the UK and Russia at the time.

The Russian approach to information warfare or 'hybrid warfare' can be seen to be in line with older Soviet thinking, with information playing a vital role in state governance. This is reflected in the 'Gerasimov Doctrine' issued in 2013 by the Chief of Russia's Armed Forces, General Valery Gerasimov, which calls for a mixture of military and non-military means when pursuing political goals. Operations are to exploit ambiguity and take place below the threshold of 'war', potentially targeting all vital parts of a society (Bartles 2016). As Connell and Vogler (2017) summarize, "Moscow perceives the struggle within 'information space' to be more or less constant and unending".

Within the Russian 'information warfare' landscape, cyber-operations play a greater role in Russian military operations, and the Kremlin has

signalled its intention to strengthen and bolster these capabilities (Connell and Vogler 2017). During its conflict with Ukraine, Russia has employed several cyber-weapons in combination with conventional proxy forces. This has provided Russia with the opportunity to refine its cyberwarfare techniques and procedures, and also to demonstrate its capabilities. In some ways, the conflict in Ukraine can be said to have served as a testing bed for Russian capabilities and as a basis for signalling these capabilities in a form of deterrence (Greenberg 2017c).

Russia has in sum been assuming a more assertive cyber-posture, as shown by its readiness to target critical infrastructure systems and conduct espionage operations 'even when detected and under increased public scrutiny' (Connell and Vogler 2017). Increasingly, Russian cyber-operations targeting Western interests are conducted within the strategic objectives of gathering intelligence and support, as well as to influence operations to support military and political objectives and "continuing preparation of the cyber environment for future contingencies" (Clapper 2016). Yet, it is important to differentiate between the different actors within Russia to fully understand the possible threat.

Organizations, agencies and cyber-warriors

Within the Russian military, the Federal Security Service (FSB) is the lead actor for coordinating disinformation campaigns. It maintains and operates SORM, the state's internal cyber-surveillance system, while Directorate K of the Ministry of Internal Affairs (MVD) focuses on cyber-crime. These agencies are central in setting the parameters of Russian cyber-doctrine, and have responsibility for coordinating most internal and external cyber-operations of the state (Connell and Vogler 2017). Cyber-concerns under the purview of the military had been restricted to operations where cyber-operations overlapped with the field of electronic warfare. However, in 2013 the Kremlin announced that it would create a cyber-unit in the military with responsibility for offensive and defensive cyber-operations, as well as a cyber-research and development agency. The current status here is unknown.[3]

Cyber-hacker groups are fundamental to Russia's cyber-operations,

[3] According to Connell and Vogler (2017), official sources in the Russian MOD reported that the budget for this agency for 2013 amounted to 2.3 billion Roubles ($70 million).

although proving the connections between such groups and the government is difficult. The Russian government has denied sponsoring any hacker groups, but several groups have been found to be connected to Kremlin.[4] In recent years, these groups have been given many different names by various threat and intelligence analysis companies and national intelligence services. However, many of these groups are the same, and can be placed into five groups that are key actors in Russian cyber-operations:[5]

1. 'The Dukes', or as they call themselves: 'Cozy Bear'. Officially named APT 29 by the US government, and have conducted strategic operations since at least 2008. The Dukes show clear signs of major long-term state backing, in their size and capacity, and are believed to be linked to the FSB.[6]

2. 'Fancy Bear', or APT 28 (Tsar team), 'Sofacy' or 'Pawn storm', has been found to be linked to the Intelligence Directorate (GRU), the intelligence agency of the Russian Ministry of Defence (FireEye 2014).

3. 'Energetic Bear', also called 'Crouching Yeti' or 'Dragonfly', has since 2010/2011 frequently been held to be the perpetrators of targeted attacks against CNI and industrial systems (Kapersky 2014; Symantec 2014).

4. 'Sandworm' or 'Telebots', 'Black Energy' or 'Electrum' is a group recent in focus, and has been named by some as the perpetrator of the 2015 and 2016 Ukrainian blackouts (FireEye 2016).

---

4 Russia is not unique in this regard: China, Iran, North Korea, and other cyber-adversaries have been known to outsource their operations to non-state actors.

5 This is not an exhaustive list of all the various names, aliases and groups associated with Russian cyber- operations. Some of these have at times been identified as the same group, or multiple different groups. In fact, one should be cautious about the many security companies and government institution attributing cyber-attacks to different groups, as their motivations and capabilities may vary. We list these groups in order to highlight that the actual operations are being performed by different actors, with different methodologies and motivations, as well as differing affiliations with and within the Russian state. In total, these agencies are capable of undertaking some of the most technically advanced computer-network operations in the world.

6 For more on the group, see for instance F-Secure 2011.

5. 'Turla Team', or 'Snake', 'Uroburos' or 'Venomous Bear' was first identified in the late 1990s, and use a variety of operations from spear-phishing, zero-days vulnerabilities, custom malware etc. and are known to target energy, defence, telecommunication and government sectors (FireEye 2018).

	Aliases	**Active since**	**TTPs**	**Targeted sectors**
APT28 (Tsar Team)	Fancy Bear, Sofacy, Pawn Storm	2008	Spear-Phishing, custom malware. Zero-day vulnerabilities, watering holes, credential collection, data theft	Government, defence, media, hospitality, construction, non-profit, technology
APT29	Dukes, Crazy Bear	2008	Spear-Phishing, watering holes, custom malware, zero-day vulnerabilities, high operational security, data theft	Government, think thank/NGOs, hospitality, finance, pharmaceutical, legal
TURLA TEAM	Snake, Uroburos, Venomous Bear	Late 1990s	Spear-Phishing, watering holes, possible human-enabled operations, zero-day vulnerabilities, custom malware, satellite C&C, very high operational security, data theft	Defence, government, energy, transportation, pharmaceutical, manufacturing
SANDWORM TEAM	Telebots, Electrum, BlackEnergy	2011	Spear-Phishing, custom malware, zero-day vulnerabilities, data theft, data destruction, physical impact	Energy, defence, telecommunications, finance, government, transportation
KOALA TEAM	Energetic Bear, Dragonfly	2011	Spear-Phishing, watering holes, poisoned software downloads, SCADA scanning, data theft	Energy, research, pharmaceuticals, technology

Sources: Estonian Foreign Intelligence Service (2018), FireEye (2018).

All five groups work on cyber-operations with some connection to the Russian government and conduct extensive espionage and sabotage actions against foreign states. Their links to the government vary, and analyses differ regarding these groups' connections with each other

and with Kremlin. However, all work internally and externally on highly advanced espionage and sabotage attacks against Critical National Infrastructure (CNI).

Other actors

Within the current geopolitical landscape and threat assessments, Russian actors are deemed to be the most likely perpetrators as to potential sabotage operations against the Norwegian petroleum sector. However, other actors should also be taken into account.

Sophisticated cyber-adversaries today include China, Iran, and North Korea (Cilluffo, 2016). Iran has expanded its cyber-capabilities, as documented in the 2014 Cylance report 'Operation Cleaver'. Similar developments have taken place in North Korea, which has been identified as the culprit involved in the 2014 Sony Hack and the 2017 WannaCry-worm (Zetter 2016; BBC 2017b). The fact that 'rogue states' are developing offensive cyber-capabilities is indeed worrisome, as they might be expected to have a lower threshold for using them (Schia 2017, 6). Moreover, such actors appear to be less concerned with conducting targeted attacks, thus causing wider spread, as was the case with WannaCry. Also, China has proven cyber-capabilities, and a history of digital espionage in Norway – but a scenario where political tensions between Norway and China escalate to the point where sabotage of CNI becomes relevant has been deemed unlikely in the current climate (PST 2017).

States may use their own military and intelligence services to conduct cyber-exploitation, but are increasingly acting through proxies to whom they may provide funding or other tactical support (Maurer 2015; Matthews 2015). This complicates attribution further. Foreign states and their proxies are joined by a range of other cyber-threat actors, including criminal enterprises, hacktivists, and terrorists engaged in malicious cyber-activities (Clapper 2016).

In addition to state (sponsored) actors, 'cyber-terrorists' and 'hacktivists', non-state actors using digital means to further their agendas have shown some instances of politically-motivated low-level digital attacks (like the 2006 DDoS of *Jyllandsposten)*. These campaigns have lacked the sophistication needed to take the step from low-level disruption to more targeted and damaging actions (Archer 2014).

However, developments like the 2017 WannaCry attack, which saw ransomware operations used against CNI, could change this (Symantec 2017a).

Thus far the resources and expertise needed to launch digital campaigns that could cause physical damage or severely disrupt infrastructure, have remained in the hands of a few states with expansive capabilities. However, recent developments could indicate that also this may change.[7] The main point is that there are other actors out there that are important to note, which are crucial to include for a holistic threat picture. The actors are many and varied, and thus the threat picture as well.

[7] One noteworthy example is the theft and subsequent sharing of cyber weapons developed by the NSA, which made possible campaigns like the 2017 WannaCry-campaign. See Shane, Perlroth and Sanger 2017.

2. Digital threats: Illustrative cases

Threats in cyberspace come from actors and states with a wide variety of attack-areas of differing scales and sizes. Security in cyberspace is a vast field, and protection against digital threats covers an extensive range of incidents and threats. To comprehend and deal with this landscape, we subdivide cyber-attacks against CNI into three levels:[8]

Top level: The large, rare and potentially extremely harmful, cyber-attacks that cause physical destruction, perhaps loss of life – 'cyberwar'

Middle level: Cyber-espionage using digital tools and weapons to extract information and gain advantages in the international arena. These attempts do not meet the definition of 'war', and can range from influence campaigns to disruption and to espionage. Such espionage may be used for sabotage later, as a stepping stone to the top level.

Low level: What most companies experience in some way or form almost daily: The routine cyber-criminal activity seeking cheap profits through illegal gains. Examples include scams (of various forms) for money.

This report focuses on the large sabotage operations found in the top-level division, and to some extent large disruptive incidents that – while not resulting in physical destruction – might have impacts at the nationwide level. Thus, we do not comment on practices in place for combating for instance cybercrime. However, there have been notable

8 The response of the National Security Authority (Nasjonal Sikkerhetsmyndighet – NSM) to a cyber-attack depends on its size and level of seriousness. In the report 'Comprehensive ICT risk-assessment 2017' NSM proposes dealing with digital incidents along two separate 'tracks': one if the incident threatens, or might threaten, critical societal functions or infrastructure; and another track if this is not the case. This indicates that digital incidents are handled differently depending on how they are perceived in the early stages: if CNI or societal functions are not impacted, resolving the crisis will depend on the company that is affected – a point to which we return.

examples of incidents that are criminal in nature and with potentially large nation-wide effects,[9] or where nation-states have camouflaged disruptive campaigns as criminal enterprises.

The differentiation between these types of attacks is not as clear-cut as often presented. To illustrate the difficulties in managing and dealing with cyber-attacks and their complexity, we draw on three cases from the Ukraine conflict 2015, 2016 and then from 2017 to illustrate the complexity of dealing with a large-scale cyber-attack. As Ukraine is viewed as a testbed of Russian strategic usage of cyber-weapons in a political escalation, these cases can serve as a good indicator of what it is reasonable to expect and how Russia operates in such a situation. The two first cases are clear-cut examples of sabotage of CNI; the third one shows how cyber-operations can be targeted. The third case also displays the grey zone between sabotage, disruption, and criminal activity exploited for political gain.

Top level: Digital sabotage of Ukraine's electricity sector

Since 2014 a flood of digital attacks has hit Ukraine. While there is yet no comprehensive summary of the attacks, a reported 6500 cyberattacks over a two-month period indicates the scale of the problem. Attacks have been targeted at the whole spectrum of Ukrainian society, hitting sectors such as the military, the media, finance, politics, and energy. As to the energy sector, the main attacks were two separate occasions where electrical infrastructure was targeted in both 2015 and 2016 (Greenberg 2017c).

In 2015, Ukraine experienced a series of attacks that leveraged a malware known as KillDisk, which renders computers useless or 'bricked', and a Trojan called BlackEnergy. The attacks hit a range of companies in different sectors, including power companies in December 2015. The Black Energy Trojan enabled the hackers to gain an initial foothold in the systems, with the initial infection apparently occurring through a false email containing a Word attachment with said Trojan. By spreading through the company networks, which were not properly segregated, the hackers managed to infiltrate the Virtual

[9] A recent example is the Equifax hack, where the social security information of over 143 million Americans was stolen. See for instance Riley: 'The Equifax hack has the Hallmarks of State-Sponsored Pros', 2017.

Private Network (VPN) connecting the computer systems with the digital control-systems that ran the physical machinery. By cloning the software used to run the control systems, the hackers could operate the computer systems as if they were present in the power plant. At another plant, they had taken over the actual cursor movements while simultaneously locking the engineers out. This allowed the hackers to open the circuit breakers as if they were legitimately in control; the second phase of the attack shut down the parts of the servers that functioned as 'translator' or connecting link between the actual machinery and the computers used for remote communication with the equipment. Finally, the computers of the power plant were shut down using KillDisk, and the battery backup that gave electricity to the power plant was taken out

The 2015 attack depended on insufficient security practices and poorly configured networks from the Ukrainian operators. The control systems in the electricity systems were directly accessible from Windows Remote Desktops, so the attackers could shut down production without having any specialized competencies as to the layout of the industrial systems. While the attack depended on networks that were not properly segregated, as well as poor firewall configurations, the relative lack of digital sophistication meant that the facility could be run manually by disconnecting the remote desktop, thereby limiting the impact and duration of the blackout.

The 2016 attack showed much greater sophistication, displaying in-depth knowledge of the industrial systems in use.[10] Whereas the 2015 incident had exploited outdated modes of protection, the industrial systems targeted in 2016 had been recently renovated through EU funding and were highly modern. The target of this attack also served a more crucial function: this time the attackers infiltrated a transmission station with a crucial role in the Ukrainian electrical grid. The attackers had also created malware able to send commands directly to the control systems, creating a far more potent weapon that could utilize industry protocols to execute its commands. From one year to the next the hackers – assumed to be the same group – had evolved, demonstrating advanced capabilities by utilizing specialized tools

[10] Many of these were brand new, had been supplied by the EU, and are the same as used throughout the Union.

dependent on intimate knowledge of the control systems and their protocols. The malware, analysed by security firms ESET under the name 'Industroyer' and Dragos under the name 'CrashOverride', has been identified as the second-ever malware aimed at destroying physical infrastructure. Its modular design makes it possible to reuse the core functions to target a wide set of industrial systems. In both instances, but with the 2016 attack in particular, security researchers have concluded that the attack had the potential to cause far more severe outages, and that the attacks were aimed mainly at demonstrating the hacker's capabilities (Dragos 2017; ESET 2017; Greenberg 2017*c*).

These incidents are somewhat transferable to a Norwegian context and level of security. In the wake of the 2016 incident in Ukraine, the security company Symantec released a report detailing how a similar level of intrusion in, and control over, critical infrastructures had been detected in US and European energy companies (Greenberg 2017a). The nature of the malware used in the 2016 hack is such that it could be configured to target other industries. Doing so, however, would be complex, and would require extensive knowledge of the industry in question to be functional. While an effective tool of sabotage, digital weapons also necessitate significant knowledge about industrial processes to be effective.

This is a crucial element in most known (and hypothesized) instances of industrial systems sabotage: the need for in-depth knowledge not only about the IT aspect of leveraging a campaign, but also about the specific industrial processes and configurations. Partly because this combination of technological savviness and industrial know-how is required, concerted campaigns achieving physical destruction through digital means have thus far been available only to nation states, and are likely to remain so for the foreseeable future (Dragos 2017).

A second lesson to draw from the attack is the fact that 'passive' defences are becoming increasingly superseded as a stand-alone solution to the more advanced digital threats, and must be complemented by more active measures (ESET 2017; Dragos 2017; National Cybersecurity and Communications Integration Centre 2017). Digital attacks against critical infrastructure are both feasible and have

their uses. Taking down the electricity grid of a region of Ukraine that was *not* involved in the ongoing hostilities showed that the attacker (presumably Russia) had the ability to cause harm even in 'safe' parts of the country, while simultaneously avoiding escalation of conflict. That the malware could be used against other industrial systems shows that this attacker has the capability to target industrial systems in other countries if a situation arose where this might be relevant. Furthermore, the attack appeared to be constructed in such a way as to avoid spill over into neighbouring states, avoiding the electricity grid that was connected to gas deliveries from Russia through Ukraine to its neighbouring countries. Cyber-attacks in a hybrid-war scenario are seen to be employed to avoid escalation by unnecessary provocation, and the use of digital weapons to cause physical harm is confined primarily to situations of crisis or hostilities.

These examples were instances of physical sabotage through digital means – but physical destruction is not the only (or main) way of harming state interests through digital attacks. In the following, we assess a case where digital attacks brought disruption and economic loss, while avoiding physical sabotage.

Middle level: NotPetya: Weaponized ransomware

Ransomware operates on a model where a computer and its files are encrypted and taken ransom, followed up by a demand for payment in cryptocurrency to decrypt the computer. In 2017, what appeared to be a ransomware attack hit many businesses in Ukraine, encrypting their files and demanding ransom. Initially the motive was perceived to be financial, as the hackers promised to decrypt the files once the ransom had been paid – a mode of operation increasingly used among cyber-criminals worldwide.[11] The malware, under many names,[12] spread rapidly through a long list of businesses. However, it soon became evident that the attack was not one of ransomware, as the payment method proved to be non-functional. In this case (which we refer to as NotPetya), the business model was never intended to work. This

11 For more on this trend, see: TrendMicro: 'The Next Tier: 8 Security predictions for 2017'

12 like Petya, ExPetr, Goldeneye and NotPetya.

indicates that the attack was not a ransomware effort, but a worm that wiped data from the hard drives of infected computers.[13]

Further investigation revealed that the attack had spread mainly through the accountancy software MeDoc.[14] Ukrainian law stipulates that MeDoc is one of the two accountancy software's to be used by businesses operating in the country. This allowed the attacker to ensure the goals of spreading rapidly to key Ukrainian businesses and government agencies. This further indicated that the attack was not criminal ransomware, but a more targeted campaign aimed at hitting the Ukrainian economy. About 80% of the afflicted companies were in Ukraine, and the remainder were contaminated through their affiliation with Ukraine (Lunde, 2017). Another indicator that Ukraine as such was the intended target was the timing: The attack started the day before Ukrainian Independence Day (Kramer 2017). The targeting of the attack had the bonus of mostly affecting Ukrainian businesses, not everyday private computer users, which magnified the economic impact (Kaspersky 2017).

The hackers had infiltrated MeDoc some time before the attack took place, and at one point the hackers had sent out a 'tainted' software update to all Medoc's customers. Investigations have indicated at the hackers infiltrated other companies as well, before settling on MeDoc as the vector for ensuring that the worm would spread as widely as possible. As MeDoc customers performed what seemed to be a routine software update they were in fact installing the malicious components on their systems. From there the malware spread laterally through the networks: when it succeeded in infecting a computer with sufficient administrative privileges it leveraged weaknesses in the windows system to install the malware in all the computers it could access. This allowed for the rapid spread of the malware throughout office systems (Greenberg 2017b; Cherepanov 2017).

As the NotPetya case shows, trying to protect against digital attacks is a fluid and complicated landscape to be deal with. The way NotPetya spread made it hard to identify and filter using commercially available security solutions like antivirus software: such an attack requires other

13 For additional information on NotPetya, see for instance The Grugq (2017).

14 There were other vectors, such as the leaked NSA-exploit EternalBlue, but the MeDoc update was responsible for the brunt of the infections.

and more complex types of defence than merely filtering data for known malware signatures. The defences that might work, like human threat-detection, are more expensive and complex. Furthermore, NotPetya's utilization of an accountancy system as the vector of attack is illustrative of the difficulty in creating policy that can encompass all possible vulnerabilities. The idea that an independent software firm is to be regarded as a 'critical' component of a nation's digital defences would strike many as odd – but the software provided by MeDoc was a crucial part of the digital ecosystem in the Ukraine, providing a key service to much of the country. The ability of digital malfeasants to utilize a path of least resistance ensures that defence will always have to been conducted in depth.

Cyber-operations can camouflage themselves as criminal activity. The NotPetya attack was skilfully crafted: it managed to hit Ukraine broadly, hitting a long list of companies, while limiting the spread of malware to other states.[15] Furthermore, it targeted not industrial control systems, but office systems, which are more accessible to intruders. By camouflaging a cyber-operation as a criminal enterprise (albeit unsuccessfully: this attack has been attributed to Russian actors), the attackers kept the political costs and risks of escalation lower than in the case of physical sabotage. The broader tactic of camouflaging state-led campaigns as criminal enterprises complicates attribution and therefore also response.

***

The three cases illustrate the difficulties in dealing with cyber-attacks that become questions of national security. They further serve as an indicator of the threat picture and Russia's capabilities and strategies in a hybrid attack. In additions, the cases show how definitions and separation of types of attacks becomes blurred in

15 However, multinational corporations, such as Maersk, were hit hard globally as a result of the attack on its systems in Ukraine, with an estimated loss of USD 300 million. See Reuters (2017) "Cyber 'Worm' Attack Hits Global Corporate Earnings".

reality: sabotage of critical infrastructure might begin by exploiting the grey areas between espionage, disruption, and criminal activity, before the actual sabotage occurs.

While the private sector is on the front line of defence, cyber-threats, attacks, and weapons cannot be examined in isolation from the political context (Rid and McBurney 2012). Large-scale sabotage operations against CNI are possible, and ensuring protection is crucial. However, protecting CNI and strategic sectors is not only about preventing large-scale catastrophic attacks: Such defence needs to incorporate a comprehensive approach to a wide range of challenges. Achieving such flexibility in facing cyber-threats requires good cooperation between the public and private sector, and a maintained holistic threat picture. With the technological evolution proceeding at a rapid pace, an adaptive and agile response system in the industry is called for.

These cases have illustrated some broader challenges to the energy sector as regards protecting systems against cyber-attack. But to what extent is this relevant for the Norwegian petroleum sector? In the next section we examine some specific vulnerabilities in the Norwegian petroleum sector, and the challenges related to prevention and response.

3. Digital vulnerabilities in the petroleum sector

Within the petroleum sector there is wide range of properties and functions – production facilities, pipeline and transportation systems, energy supply, offices – that to various degrees are digitalized and online, and thus vulnerable to cyber-attacks.[16] In this report, the focus is primarily on vulnerabilities that can impact Norwegian petroleum export.

In order to protect core functions in the petroleum industry from digital attacks, the digital control and safety systems are separated into several zones, with firewall-protection between them. As illustrated in Figure 1 below, the different computers, networked data communications and graphical user (zone 2) are separated from the corporate networks (zone 4). The systems that control the industrial processes are located in zone 1. A separated part of zone 1 contains the safety instrumental system that close and shut down the whole plant in case of emergency. The different core processes (zone 0–2), are protected by firewalls and a separate so-called demilitarized zone (DMZ). The DMZ allows for users of the administrative network to access information from the protected network without actually accessing the protected network itself. Taken together, this zone architecture is designed to enhance security and reduce potential of digital intrusion.

While zone thinking isolates the number of actors that have access to the different systems, subcontractors and vendors may be given access to dedicated functions in corporate network utilizing normal security functions. For remote support to the digital control systems, internal resources and external vendors may be given access to relevant functions in computers located in the DMZ.

---

[16] Tor Olav Grøttan, "Digital attacks on Norwegian Petroleum Infrastructure – Vulnerabilities and Consequences", Presentation at NUPI 02.02.2017

A potential digital sabotage of the petroleum infrastructure would in most cases need to target the industrial control systems in zone 0–2. If the defence mechanism is bypassed or hacked, the control system can be interfered with – by delaying or blocking the flow of information, or by making unauthorized changes to the control system (NOU 2015:13, 146). However, provided that the systems described above are in place, such an attack would be complicated and resource demanding for a potential aggressor. It would require advanced skills, sophisticated malware and detailed intelligence about the industrial control system that is being targeted.

Nonetheless, even with zone thinking in place, no system is 100% secured. The systems have several potential access points that could be utilised. As mentioned, all digital systems are reliant upon various suppliers of digital services. It is a challenge for any corporation to have full oversight and security control of all such digital supply chains. Sub-contractors may at times be given access to vital systems to conduct updates, maintenance etc. This could also be an access point for malicious actors. Furthermore, employees, with or without intent, can be used to gain entrance to critical systems. This way even firewalled and air-gapped systems can be compromised.[17] Yet, despite these potential attack vectors, such attacks are rare, and have so far only been conducted by states with the required intent, skills and capabilities.

[17] The Stuxnet attack against the Iranian nuclear enrichment facility Natanz illustrates this. The system was not connected to the Internet, but nonetheless attacked through the laptops of some of the personnel servicing the system.

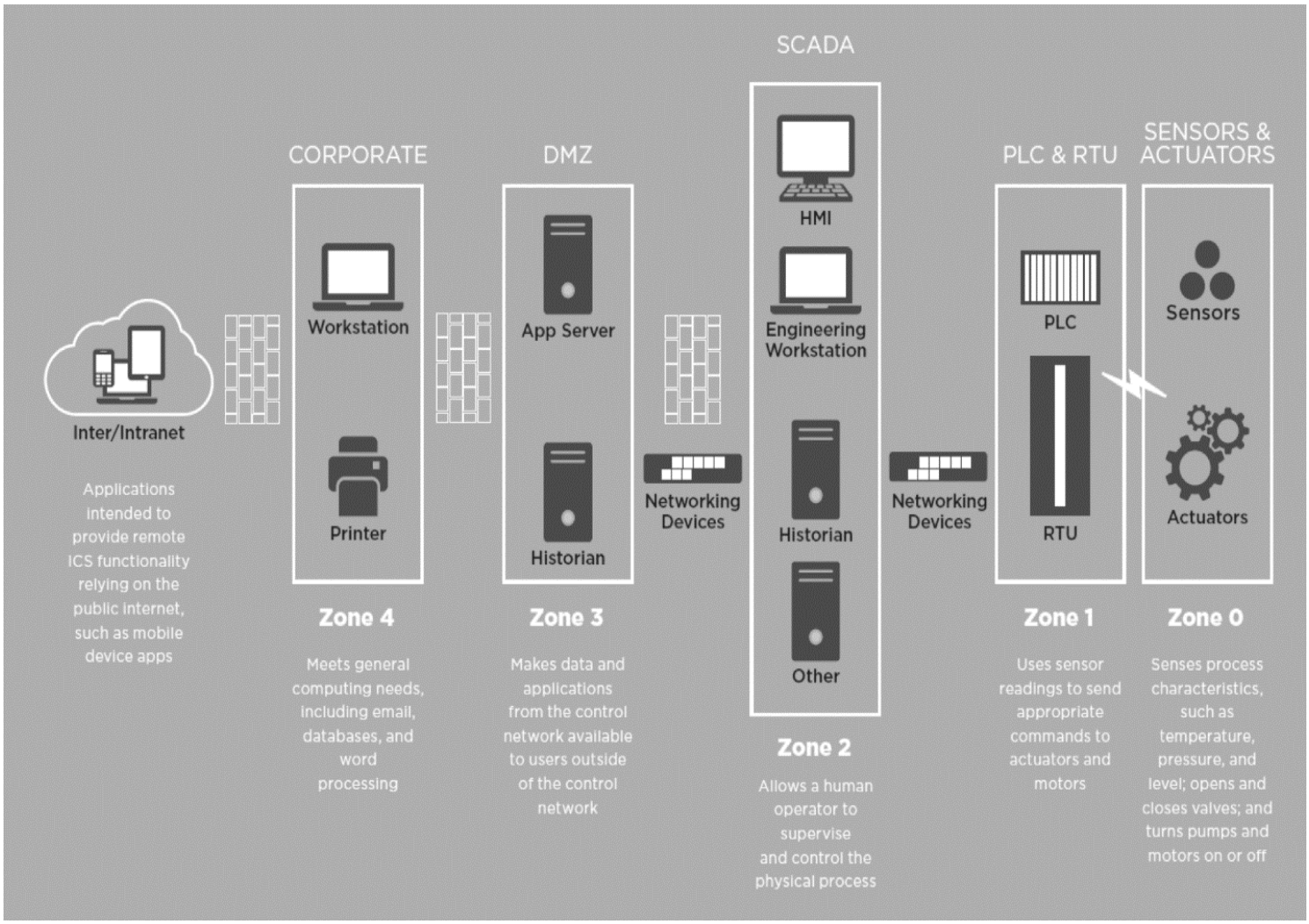


Figure 1. From PSA-brief (2017) “IKT-sikkerhet: Tilsyn med operatører og redere”, based on FireEye Inside intelligence (2016) “ICS Vulnerability trend report”.

Office or corporate systems (zone 4), however, are more frequently attacked – in the petroleum industry as in any other sector. Sophisticated users have numerous digital weapons that may be applied to sabotage or shut down vital office systems. This can sabotage or undermine production in at least two ways. Firstly, a shutdown in office systems could negatively impact production indirectly and over time. If 'office tasks', such as staff rotation plans, procurement, supply and service is hampered with, production may be reduced or stalled.[18] Secondly, cyber espionage or attack against office networks may be used to gain access to industry networks (zone 0–2), by for instance stealing passwords, manuals etc.

Such attacks require far less sophistication than direct on the control systems. It requires less intelligence, competences and there is a larger attack surface. Hence, office or corporate systems are often considered a weak link in industry security.

The next part of the report outlines the roles and responsibilities in protecting against cyber-attack in Norway, and aims to illuminate where the grey zones and problems arise between the sector and government in dealing with a potential cyberattack.

---

18 The potential impact of targeting office systems in the petroleum sector has been demonstrated in the digital attack 'Shamoon' on Saudi Aramco. The attack, widely believed to be the work of Iran, 'bricked' - or made useless – an estimated 30.000 computers in the company. While no industrial systems were affected, and no official cost estimates exist, the disruptive effects are considered to have been significant. For more on the Shamoon/Distrack-attack, see for instance Lucas Kello "The Virtual Weapon" (2017) and the International Institute of Strategic Studies (IISS) "The Cyber Attack on Saudi Aramco".

4. Regulation and responsibilities

It is first and foremost the responsibility of each individual company to secure its own digital systems (Petroleum Act, 1996, §9.3). Yet severe digital attacks of the kind we discuss in this report will have national implications as well. This means that the government and the relevant agencies have a role to play in detecting, preventing and responding to such attacks. A seamless transition between private sector companies to authorities will require a holistic threat picture, clear areas of responsibilities, and good procedures that are exercised regularly. This is hardly the case today.

To clarify the challenges in division of responsibility within cybersecurity in the Norwegian petroleum sector, this report divides digital security into two parts: roles and responsibilities in *preventing* digital attack, and roles and responsibilities *managing* digital attacks when they occur. Next, we will examine the roles and responsibilities of the various actors, according to their mandate, and then we turn to some key challenges in prevention and response.

Here it must be borne in mind that the regulatory terrain is currently changing. There are several ongoing processes that are relevant for the prevention and response to digital incidents in the Norwegian petroleum sector. Firstly, there is the new Security Act, and four associated sets of regulations that are currently being drafted. Secondly, a Framework for digital incident management (RHI) is under development.[19] The Ministry of Justice and Public Security is also working on a new national strategy for digital security and an accompanying action plan.

The petroleum sector is currently not defined as CNI, which means that the sector is not prioritized by the authorities when it comes to security. However, the new Security Act stipulates new procedures to

[19] Prop. 153 L (2016–2017) "Lov om nasjonal sikkerhet (sikkerhetsloven)". "Rammeverk for håndtering av IKT-sikkerhetshendelser" (RHI) is not yet publicly available. This report is based upon a draft dated 07.12.17.

define or incorporate something as CNI, or so-called 'basic national functions'.[20] The change in emphasis to functions in the new Security Act has led to an expectation that the petroleum sector will be partly incorporated due to its importance for the national economy, yet the final decision will be taken by the sectorial ministry (Ministry of Petroleum and Energy). The associated regulations are likely to define how this is to be protected, and by whom. However, at the time of writing it has not yet been determined what parts of the petroleum sector this eventually will involve.

The RHI is to clarify the roles and responsibilities of the private companies and various authorities when a digital incident occurs, and is mainly intended for those companies and systems that have been designated as CNI under the Security Act. These regulations are at different stages of revision. However, as long as the petroleum sector is not considered CNI, the regulations and guidelines given by the Petroleum Safety Authority (PSA) provide the main principles regarding ICT security in the sector.[21] The section below is therefore based on the current legislation and regulations, but the discussion also considers the draft RHI and the new Security Act when relevant.[22]

Relevant actors in cybersecurity in the petroleum sector

Various actors are involved in securing the Norwegian petroleum sector:

Ministry of Justice and Public Security holds the cross-ministerial coordinating role, through relevant regulations and legislation. It serves as the coordinating body between the various ministries and ICT security in the civil sector. This includes national policies for both the public and the private sector.

Ministry of Petroleum and Energy holds the overall responsibility for the management of petroleum resources on the Norwegian

---

20 The New Security Act use the term 'skjermingsverdig infrastruktur', and also 'grunnleggende nasjonale funksjoner' ('basic national functions') to incorporate more than just physical infrastructure. For the sake of simplicity, we have nonetheless used the abbreviation CNI in this report.

21 See for instance PSA "The Framework Regulations".

22 Interviewees tended to differ regarding their reference to the ongoing processes: some often referred to the new Security Act, while others based all replies on the current situation.

continental shelf. The ministry is to ensure that petroleum activities are conducted in accordance with the guidelines issued through the Petroleum Act (NOU 2015:13). The ministry will also decide if objects in the industry should be covered by the Security Act.

The Petroleum Directorate (OD) is responsible for managing the petroleum resources on the Norwegian continental shelf. The OD reports to the Ministry of Petroleum and Energy, and functions as the directorate for the Norwegian Petroleum sector. It is responsible for the security of the data and information collected from the petroleum sector from seismic surveys, well data and production volume reporting (Norwegian Petroleum Directorate 2017; NOU 2015:13).

Ministry of Labour and Social Affairs is the ministry responsible for the health and safety of the petroleum sector, as well as security, including cyber security.

The Petroleum Safety Authority (PSA) is an independent authority situated under the Ministry of Labour and Social Affairs and functions as a supervisory body with responsibility for safety, preparedness and working environment in the Norwegian petroleum sector. PSA is responsible for conducting supervision in the petroleum sector.

The National Security Authority (NSM) is a cross-sectoral professional and supervisory authority within the protective security services; it is to maintain the national security assessment picture. NSM shall primarily contribute to state security and societal security, through preventive measures against espionage, sabotage and terrorism. NSM is also the supervisory authority for objects regulated by the Security Act, but can inform and advise other actors as well (Prop. 151 S, 2015–2016)

NorCERT is the National Computer Emergency Response Team; it is to coordinate the response to digital incidents. NorCERT is a part of the NSM and assists in maintaining the overall assessment picture of the threat landscape. It also serves as the coordinating entity of the CERTs and is a response environment.

Sector Response Teams (SRM) is a measure by the government to establish response teams, or CSIRTs (Computer Security Incident Response Team) in the various governmental sectors. These are to

support their individual sector in case of digital attacks and to ensure flow of information to and from the central authorities (NSM/NorCERT). Each sector is to define its needs and most efficient way of organizing these SRMs. At a minimum the sector ministries are to establish points of contact both within the sector and towards NorCERT to facilitate exchange of information (Meld. St. 29, 2011–2012, section 9.3).[23]

The Police has the responsibility to prevent illegal activities, as well as investigating criminal activity in the digital as well as the physical domain.

The Police Security Service (PST) is to prevent sabotage and politically motivated violence (Police Act, 1995: §17). It is the intelligence and security service unit tasked with domestic intelligence, and is to collect and transmit intelligence to the public through threat assessments and cooperation with relevant actors.

National Criminal Investigation Service (KRIPOS) is the national police unit tasked with combating organized crime, as well as other serious offences.

The Norwegian Intelligence Service (NIS) is under the Ministry of Defence, and is responsible for foreign intelligence, including in the digital domain.

The Norwegian Joint Cyber Coordination Centre (FCKS) is a coordination mechanism between NSM, PST, NIS and KRIPOS in the occurrence of the most serious cyber-attacks.

The Norwegian Oil and Gas Association (Norwegian Oil and Gas) is a professional body and employer's association for oil and supplier companies engaged in the field of exploration and production of oil and gas on the Norwegian Continental Shelf. The Association works to solve common challenges for the members, including ICT security. It operates the Petroleum Industry Security Alert System **(**PISAS), which can be an important arena for information sharing in case of a digital attack.

---

23 See also "Nasjonal strategi for informasjonssikkerhet: Handlingsplan, 2012", tiltak 4.2

Challenges in *prevention*

The above-mentioned actors all have various roles and responsibilities as regards to securing the petroleum sector against digital threats. Although the division above states the overall roles of each actor, various challenges emerge in upholding the division of responsibility in threat prevention. Especially four challenges stand out in the efforts to prevent cyber-attacks in the sector. Descriptions of the challenges (below) build on interviews with various stakeholders.

Supervision

The Petroleum Supervisory Authority (PSA) holds supervisory authority for digital security in the petroleum sector.[24] In its current form, supervision in the petroleum sector differs from other sectors, being confidence-based and with flexibility for companies to achieve security in ways appropriate to the individual company. PSA does not set fixed standards or requirements, but focuses on the goal of security for the company in question (PSA, 2017a). While the regulations can refer to guidelines for 'good practices' and recommended baselines, and ISO-standards, these are not mandatory in the form proposed.[25]

The interviews revealed significant interest in the role of the PSA. While some interviewees argued for a less rigid form of supervision as advantageous, particularly regarding *safety and costs*, others expressed concerns that the current system does not provide sufficiently results when it comes to *security*. Some interviewees asked for concrete goals, targets, and standards for security with cybersecurity through regulation and legislation, yet others were concerned about an apparent reluctance to implement proposed standards, due to cost considerations. Further, concern was raised in the interviews regarding PSA's primary focus on the digital industrial systems, and a lack of supervision of office and corporate systems. It was also claimed that the PSA, when conducting supervision, primarily relies on security

[24] See PSA "The Facilities Regulations §5h" and "The Management Regulations §5".

[25] See for instance the Guidance to the Facilities Regulations §34, which mentions the Norwegian Oil and Gas guidelines for baseline requirements 104 as a recommended baseline for securing process control, safety, and support systems (PSA, 2017).

briefs by the companies, and do not sufficiently inspect operational security.

If and when parts of the petroleum sector will be considered as a critical function/infrastructure in need of protection under the new Security Act, NSM/NorCERT will also have a role in the supervision.[26] This arrangement is intended to enable the NSM to gain an overview nationally, while avoiding overlapping regulation, supervision, and confusion regarding responsibilities. It could potentially resolve some of the concerns addressed above, but could also create more confusion, as the number of government agencies with partial responsibility in the sector will increase.

Flow of information

To ensure efficient preparation (and response) to digital incidents, all parties agree on the importance of being able to share information within the sector, from the sector to the national authorities and vice versa. Companies depend on receiving relevant information quickly in order to deal with security challenges, while the authorities are dependent on information from the companies in order to form an overall picture of the situation (as shown by the 2014 attack). This information flow goes two ways: top–down from the authorities to the industry, and bottom–up from the sector to the authorities:

Top–down:

Channels of communication between the government and industry are important both in prevention and in the event of a crisis. Actors in the sector asked for more information sharing regarding the national threat picture to help them develop better risk assessments, and to be able to respond to potential threats. Furthermore, such information was said to be useful for security officers to convince the management of the importance of spending resources on digital security measures. Companies in the sector argue that they currently depend on open source intelligence and their international network to create their own threat assessments. Larger companies may receive information from foreign partners and mother companies, and are found to often rely more on these than the government to obtain information they regard as essential. Government representatives on the other hand, tended to

[26] Prop 153L, 2017, and interviews.

question the necessity of sharing of intelligence with the private sector, as the latter lack convincing arguments for the utilisation of the information. There are also legal limitations as to what intelligence services can share with the private sector.[27]

To improve this NSM/NorCERT is currently establishing a portal for information sharing of digital threats and attacks that is under development, but how it will function remains to be seen. This portal is however only for the members of the VDI-system, and will thus not cover the whole petroleum sector. [28] Warning systems such as the PISAS, where PST and PSA are represented, used to warn about threats and security incidents, could potentially also be an arena for information sharing. Regardless of these measures, the industry desires formalized and more frequent communication through established platforms. A possible model to replicate, which was highlighted by interviewees, is the security forum in the communication sector.[29]

The government initiated the principle of Sectorial Response Teams (SRMs) in 2011–2012, with the intention to better ensure the flow of information. The government stipulated that such a SRM could take the form of either a fully-fledged CERT, or a smaller response team (Meld. St. 29, 2011–2012). However, neither has been established in the petroleum sector up until now. The private sector has been reluctant to provide the required manpower for a fully-fledged CERT, while the government has been relatively passive in initiating the minimum requirement of a smaller response team. It is the responsibility of the sector ministry to establish an SRM, but this may have been complicated by an apparent confusion as to which ministry (Ministry of Petroleum and Energy or Ministry of Labour and Social Affairs) holds the primary responsibility to do so.

---

[27] According to "Instruks for Etterretningstjenesten", §16 "Oppdrag fra og rapportering til instanser utenom Forsvaret", the NIS may not share intelligence to actors beyond the Armed Forces unless so decided by the Ministry of Defence.

[28] "Varslingssystem for digital infrastruktur (VDI)", is a sensor network run by the NSM on CNI. It is nonetheless voluntary for the company in question, and based upon mutual trust. See https://nsm.stat.no/norcert/varslingssystem-for-digital-infrastruktur-vdi/ for more on VDI.

[29] EKOM sikkerhetsforum

According to interviewees, in the current absence of an SRM, the industry expresses desire for better communication with NSM/NorCERT. However, NSM/NorCERT is cautious about fostering too close cooperation, as this might undermine the (not yet formed) SRM, and the principle of sector wise responsibility on matters of security.

Bottom–up:
The flow of information goes both ways, and the authorities are dependent on information from the industry about security incidents and attacks. While both the draft RHI and the PSA regulations (PSA, 2017), state that that relevant incidents are to be reported, representatives of the industry expressed concerns about reporting, for fear of negative consequences. Examples of consequences mentioned were: that reporting could trigger inspection and impose new security measures; negative reputational effect that could lead to economic damage; and disruption of day-to-day operations due to investigation, for instance by the police. Lastly, the limited faith in the government's ability to handle incidents reduces private sector's incentives to report digital security breaches.[30]

As long as an SRM is not established, a key part of the information-sharing mechanism is not in place for those in the sector that do not have a VDI cooperation with NSM/NorCERT.

Implementation of the new Security Act, the RHI, the revised PSA Managements Regulations and the establishment of an SRM for the petroleum sector could all positively affect the flow of information between the public and private sector, both bottom up and top down. How these are implemented will therefore have a significant effect on information sharing from the sector to the authorities, and vice versa.

Supply chains and security standards
The Lysne I report (NOU 2015:13) points out that digital supply chains represent a general challenge when securing critical digital infrastructure. The dependencies of various sub and sub-sub suppliers makes it difficult to demarcate each company's responsibilities in

[30] The relevant PSA regulation was revised on 18.12.2017, adding stricter demands for reporting ICT-incidents. The interviews were conducted prior to this revision, which might in some instances influence the answers that were given.

securing their systems. There are limits to how far each actor can realistically enforce its standards and requirements throughout the supply chain.

In the digital world, skilled adversaries may turn to supply-chain attacks. Like the NotPetya attack illustrates, it is difficult to establish 100% boundaries around systems, but having a functional security baseline to raise the minimum level is important. Several stakeholders interviewed called for a broader minimum standard, raising concerns that the security work in the petroleum sector varies greatly, with especially smaller companies lagging in terms of maintaining sufficient security. Several interviewees note the need for clearer guidelines from the authorities, in the form of security standards or similar solutions. However, the sector expressed ambiguity regarding the need for digital security standards: While they acknowledged the complexities related to achieving sufficient security on their own, there is also reluctance to impose new standards due to limited resources.

Exercises

Stakeholders interviewed vary considerably in their perceptions of the cybersecurity challenges in their sector. However, all agree that exercises are essential for improving systems and cooperation to face the challenges and weaknesses involved in securing the petroleum sector. Yet, of annual exercises, few were considered to reflect the cyber-risks and challenges of the current threat landscape. Exercises such as the large-scale IKT16 involved extensive ICT attacks that hit multiple sectors and management areas (Fardal and Elstad 2017). However, this exercise was primarily focussed on the public sector and the sector response functions in relation to the NSM/NorCERT. As a result, PSA and NSM/NorCERT participated, but not the private actors in the petroleum sector. Several interviewees mentioned that there is a need for more exercises were the public and private sectors could participate together. This could help to identify weaknesses in cybersecurity and reduce the grey zones in the division of responsibilities between the various actors.

Challenges in *response*

When prevention of a digital threat or a cyber-attack fails, appropriate response measures need to be activated. If Norway's petroleum sector

is targeted by a cyberattack, several sets of response measures are triggered. The response framework to date has operated primarily at three distinct levels: that of the individual company, the relevant sector, and nationally – as relevant in the specific case. The division of responsibilities is enshrined in four key principles: *responsibility, equality, proximity,* and *cooperation*.[31] At what level any given incident is handled, depends on the scope of the attack, the possible consequences, and the wider ramifications for society (NSM 2017).

Digital incidents vary in their severity and implications. As a result, the response and countermeasures taken will vary accordingly, and there is no catch-all description of either digital incidents nor the response. Some of the factors that might impact the response are the type of company affected, the number of companies hit, which parts of the systems that are affected, the severity of the incident, and whether the company is covered by the Security Act regulations. This in turn is likely to be the result of the type and goal of the attack. For instance, while an infiltration of control and industrial systems may be considered to be severe, these types of attacks are seen as less likely to affect several companies due to differences in configuration of said systems. Incidents in office systems on the other hand would have a higher likelihood of affecting other companies as well.[32]

As mentioned, a digital incident in the petroleum sector is managed within the company, as ICT security is the individual responsibility of each company (Petroleum Act, 1996, §9.3). Each company is to have established a level of security based on their own threat and risk assessments, in accordance with the relevant regulations (Meld. St. 10, 2016–2017). A company is expected to have access to the capabilities to manage a digital incident. Therefore, it may utilize a commercial third partner for its digital security needs.[33] For the petroleum sector another factor warrants attention: As several of the smaller companies are actually branches of international companies, there may exist

---

31 In Norwegian: *Ansvar, likhet, nærhet, samvirke.*

32 For an extended debate on the trade-offs between the ability to hit several targets and the ability to cause severe damage, see for instance Rid, McBurney "Cyber Weapons", 2012.

33 As expressed in the "Framework for Managing Digital Incidents" version 07.12.2017.

significant capabilities for dealing with incidents centrally in these larger corporations.

Roles and responsibility in detecting and responding to a digital attack

While companies have the main responsibility for securing and protecting their own systems, the government is able to assist in managing, detecting and investigating the incident to varying degrees. The level of government involvement depends on a number of factors, such as the criticality of the systems affected and the larger societal impacts and whether CNI is considered threatened.[34] The following discussion is based on the NSM publication "Comprehensive ICT Risk Picture" (Helhetlig IKT-risikobilde 2017), which operates with two tracks; one for attacks on CNI covered by the Security Act, and one for other digital incidents.[35]

A. **An attack is not considered to harm CNI**: In this case, the company that detects the incident is expected to take care of the incident itself, in cooperation with existing partners. The SRM can here be contacted for guidance on how to deal with the incident. Once the attack has been stopped and the company has returned to a secure state, the company is expected to report the incident to the police for investigation, who can turn to the NSM/NorCERT for information regarding the technical indicators in connection the with criminal investigation. If a company in the petroleum sector experiences a digital incident that might impact production, PSA is to be notified in accordance with the routines for reporting security incidents (PSA 2017e § 29). If the incident impacts or disrupts oil supplies, OD is also to be notified. The PISAS forum for sharing information in the event of a security situation can be utilized if there is a possibility that the digital incident has a sector-wide impact. In PISAS, PST can also disclose

[34] Also expressed in the "Framework for Managing Digital Incidents".

[35] See also Figure 2 "When a business is hit by a ICT-incident", in NSM 2017. While this report gives a description of crisis management that should be considered correct in general terms, the management of digital incidents is likely to vary from case to case, based on the considerations of the actors involved and the estimated potential impact.

information on actors and intent if necessary. In addition, some of the larger companies have bilateral agreements with NSM/NorCERT through the VDI system (NSM 2017) .

B. **The incident detected is evaluated as an attack on CNI:** In this case, the company that detects the attack is to report it to their SRM, or NSM/NorCERT directly if no SRM is established in the sector. The SRM is to report to the NSM/NorCERT, as well as assist the company in managing the incident with the cooperation of NSM/NorCERT. The company, acting in cooperation with the SRM or any other company with which has agreements, is to work to stop the attack and secure its systems. It is also to report the attack to the police. Additional national resources might also be involved in managing the incident:

NSM is the lead authority for coordinating the national effort towards managing ICT-incidents deemed to threaten or target CNI. Further, the NSM is to take lead and report to the Ministry of Justice and Public Security, the Ministry of Defence, the FCKS, the SRM, the businesses connected to the VDI, and any other companies that are affected.

PST is to collect information on individuals and groups that may pose a threat, analyse information obtained and create a threat evaluation, in addition to investigating the case.

The Police (KRIPOS) assist in rebuilding a secure situation by handling the consequences and /or using force to stop the attack. They further work to secure the technical traces and conduct investigations. It also takes part in the work of the FCKS and report to the Ministry of Justice and Public Security, the lead ministries and the companies affected.

The sector ministries, in this case the Ministry of Petroleum and Energy, have the main responsibility for their respectable sectors, also in the event of a digital crisis. Ministries are to cooperate with their SRM to obtain a situation awareness picture, and further to evaluate the need to implement other

actions within the sector and report to the government or the lead ministry.

In this large apparatus involved from the government, NSM is likely to have a more extensive role, coordinating the response and involving other actors, e.g. the National Communications Authority (NKOM) if deemed necessary.[36] NSM/NorCERT can also play a larger role in actual management of the attack, as well as assisting in dealing with the incident in cooperation with the SRM. The Ministry of Justice and Public Security has the overarching coordinating responsibility for security in the civilian sector.

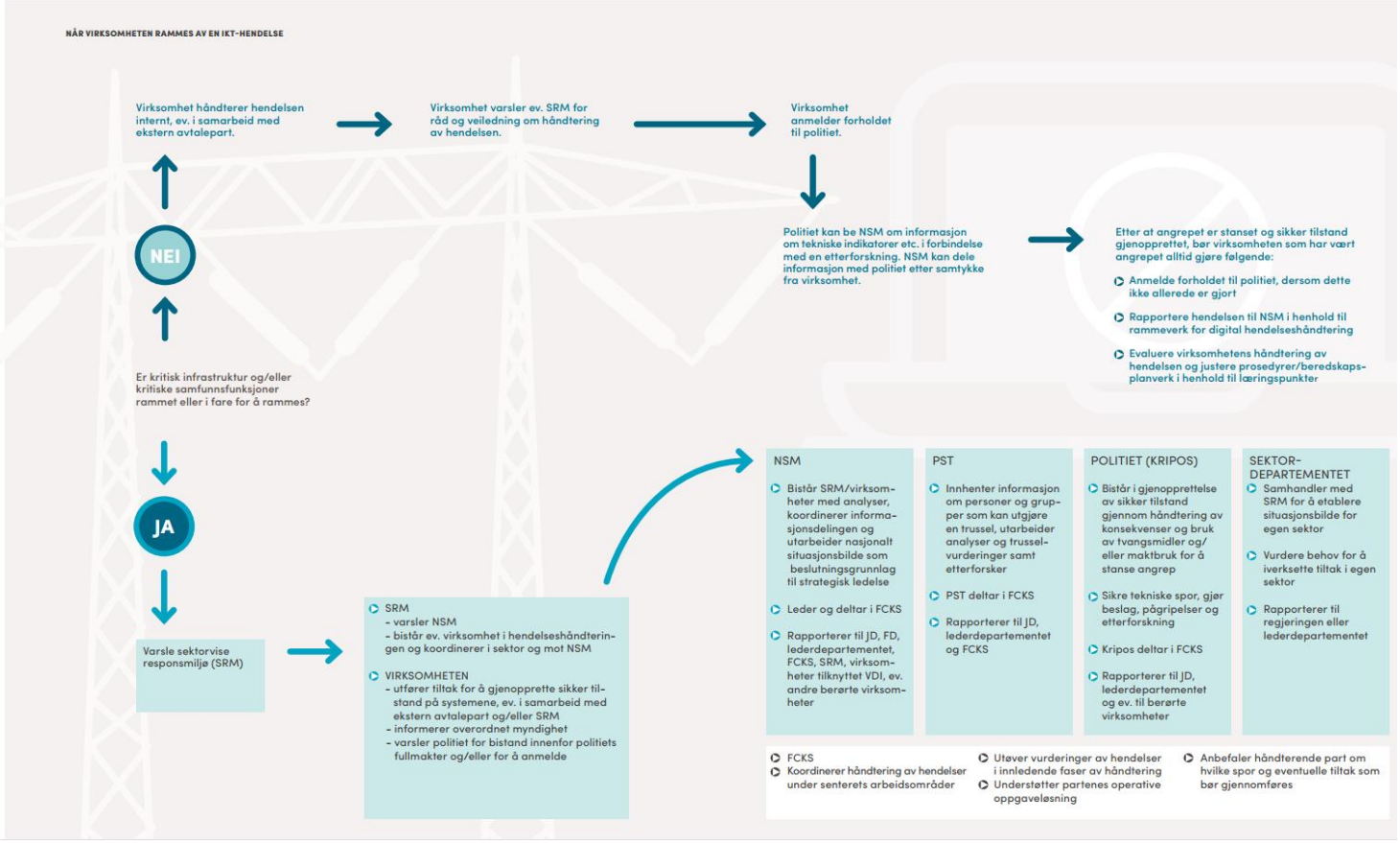


Figure 2: "When a business is hit by a ICT-incident", from Helhetlig IKT-risikobilde, NSM 2017

[36] The draft 'Rammeverk for håndtering av IKT-sikkerhetshendelser' (RHI) version 07.12.17, details these processes in greater detail.

Issues for companies handling of digital incidents

The description above is an ideal-type description of the response processes. There are, however, several practical challenges that may not necessarily be resolved through the above mentioned new legislation, frameworks and guidelines:

During the interviews concerns were raised about the abilities of companies to detect an intrusion in their systems. Understandings varied as to what was expected from them in level of system protection and deterrence. Without access to a broader situation awareness picture for Norway, the different companies expressed that they find it challenging to put ICT-incidents into a societal perspective, which they deem to hinder their ability to evaluate the scale and importance of a possible attack.

Attackers can mimic a seemingly low-level ransomware attack to achieve a strategic goal, as described. In the 'NotPetya' case, the initial attack was masked to look like ransomware, possibly to allow some degree of plausible deniability for the attacker. These types of incidents are harder to assess correctly than with cases of physical sabotage. The lack of a broader situation picture could reduce the ability of companies to assess a digital incident correctly – and that digital attack might go undetected or underreported.[37]

The ability of the NSM/NorCERT or the SRMs to detect an attack is contingent on whether the targeted company is part of the VDI cooperation. If a company is not part of the VDI, detection capacity beyond the company itself is currently limited.

Due to lack of competencies, companies (smaller ones in particular) often struggle to build up their own capacities. Being able to utilize commercial third parties can help, but correctly asses what is 'sufficient' capacities remains a challenge. Some interviewees noted the need for an authority tasked with supporting businesses in building

---

37 While this report focuses on sabotage, the problem is likely to be much more acute in the case of digital espionage, where stealth is a far higher priority than the case in disruptive or sabotage campaigns.

their own capabilities, modelled on similar efforts in, for example, Canada and the United Kingdom. In these countries, the government has established go-to-points and portals where private sector entities can get information, guidance, and advise on cyber security.

Challenges in response and the role of the SRM

In debating the role and functions of the SRM one should note that they are intended to serve a dual function. On the one hand the sectorial departments have the responsibility to establish SRM in their relevant sectors, or at the very least a point of contact between NSM/NorCERT and the sector. These are the connecting link between the authorities centrally (NSM/NorCERT) and the sectors (Meld. St. 29, 2011–2012). At the same time the sectors themselves are given considerable room to establish the types of response environments they deem necessary.

Without an SRM information exchange regarding digital threats is based on informal channels, as well as face-to-face meetings. Interviewees mentioned this as a problem, as this not would be satisfactory in the event of a crisis. In this respect the importance of routine communication and sharing of information through a public/private sector platform or annual events was noted.

KraftCERT has been proposed as a sector CERT for the petroleum sector, which could lead to beneficial synergies, due to its experience with ICS and other control systems. This could fill the need for a larger CERT with competencies on industrial systems (NOU 2015: 13). KraftCERT is formally made available for the petroleum sector (Meld. St. 38, 2016–2017), and the PSA frequently informs the industry about this option. However, there appeared to be little knowledge of this availability among stakeholders in the sector. Cooperation with KraftCERT was mentioned positively in the interviews, particularly regarding its capacity to build competencies and capacities on digital industrial systems. Yet the sector does not see this cooperation as a solution to the expressed lack of dialogue with NorCERT, nor the absence of an SRM.

General challenges in response to digital incidents

In the interviews questions were raised regarding the capacity of the authorities to deal with a major cyber-attack. There was consensus that the NSM/NorCERT's current capabilities are limited, as is its mandate

and the resources it can draw on in the event of a crisis. Some called for a possible inclusion of other private sector actors, such as Telenor, cyber security firms and SRM teams, when responding to a national attack. Some companies also lean on international resources from within their larger corporations to respond to digital threats. If and how these resources could be utilized in the event of a crisis is not evident today. As the petroleum sector is of importance beyond Norway, there seems to be a potential to enhance international cooperation with both private and public international actors.

Further, the interviewees expressed concerns about the capacity of the Ministry of Justice and Public Security, and the government in general, to take charge in case of a major digital attack. Norway's national crisis management apparatus is limited, and cross-sectoral situational awareness and command-and-control may be hampered by the strict sector-based organization of national crisis management.[38] In the case of a major digital attack on the petroleum sector, most of the actors discussed here are likely to be involved: some report to the Ministry of Petroleum and Energy, some to the Ministry of Justice and Public Security; and the Ministry of Labour and Social Affairs, the Ministry of Defence, and the Ministry of Foreign Affairs may be involved as well. As a result, and despite the overall coordinating responsibility of the Ministry of Justice and Public Security, a national response to a major cyber-attack may be slow and insufficient, and in the worst case allow the perpetrator to cause more extensive damage.

---

[38] The government has a number of coordination mechanisms for crisis management, such as the government crisis council, the crisis support unit (KSE), the government security body (RSU) and several informal cross-sectorial networks. Nevertheless, the government is frequently criticized for not having a strong enough centralized crisis management structure in place.

Conclusions

In 2017, the Norwegian Ministry of Foreign Affairs issued a white paper on International Cyber-Strategy, calling for international cooperation to prevent digital incidents that cross-national borders (Utenriksdepartementet, 2017). Cyberspace knows no national borders, nor do cyber-threats. This is important, not least in the Norwegian petroleum sector, where both national and internationally companies are involved. The sector is the largest source of income to Norway, but the borders between what is private and public in the sector are fluid. A cyber-threat to the Norwegian petroleum sector will by definition also be a threat to the sector on an international level, and vice versa. Global thinking is essential.

If the idea of an active international cybersecurity policy is to be taken seriously, the petroleum sector must be included in active, engaged cooperation on standards, threat assessments and information sharing, within and outside of Norway. The international dimension can yield important benefits in terms of knowledge, expertise and information-sharing. In today's increasingly tense geopolitical climate, Norway's position as a stabile deliverer of energy to Europe plays a central role.

Russia is Norway's main competitor in the petroleum marked and is previously found to have infiltrated Norway through cyberspace. To grasp how Russia might potentially use cyber-weapons in a tense political situation, we have examined Russia's cyber capabilities and actors, and assessed them within Russia's broader military strategic thinking. There is no doubt that Russia possesses advanced cyber capabilities, but the probability of a major cyber sabotage attack against the Norwegian petroleum sector today is deemed as low. It is here important to separate between espionage and sabotage. The probability of the use of cyber weapons to sabotage Norwegian petroleum export outside of a broader political conflict is low, as the costs most likely would outweigh the benefits. It would require a large-

scale hacking operation, imply huge political risk and would not necessarily succeed. Further, the European gas and energy market is evolving, with diversification in new suppliers and sources, and growing use of renewables. The marked may be less dependent upon fixed supply and thus less vulnerable to sudden shortage than some years ago. Still, several European countries are highly dependent upon Norwegian gas, and cannot find satisfactory alternatives overnight. Furthermore, political circumstances may rapidly change. It will be too late to build security in the midst of a crisis. It is therefore important to understand the way a potential threat actor acts, the structure of its capabilities, and how it operates, in order to construct a functioning deterrence, defence and response in Norway.

Three cases from Ukraine have served as examples in this report of digital sabotage against CNI: two where the power grid in Ukraine was shut down due to a cyber-attack, and then when the Ukrainian software company MeDoc was compromised, which resulted in a fake ransomware wiping hard drives and crippling large parts of the Ukrainian economy. Such risks, which can spread and be inherited across companies and sectors, are especially prevalent in the digital domain. They also illustrate that significant weaknesses may be located outside core functions. It may be in the corporate office network, or in key functions these rely on. This calls for action beyond designating key companies, infrastructures, or systems as 'critical', and thus warranting greater protection. The fact that also CNI relies on international digital supply chains and sub-contractors demonstrates the complexity of delaminating exactly where the lines of responsibility go.

This report has identified some of the key challenges within the division of responsibility in case of a major digital attack on the Norwegian petroleum sector. In short, the following challenges are considered as most pressing:

- Unclear roles and expectations of public sector agencies
- Different expectations related to supervision and security standards
- Insufficient information exchange between public and private sector
- Limited human resources and capacity

First and foremost, it is the responsibility of each company to secure its own systems. The national authorities become involved primarily when an installation or a function has been designated as CNI (wholly or partly) under the Security Act. As the petroleum sector this far has not been defined as CNI, efforts have been put in place to clarify the differing roles and responsibilities in protecting the petroleum sector against digital attacks. Uncertainties nonetheless remain. This applies both to the establishment of preventive measures and to questions about at what stage the authorities are to be involved in handling a digital attack, and what such involvement would entail. There remains an unresolved grey zone between what petroleum-sector companies can reasonably be expected to manage on their own, and how large and significant an attack should be before the authorities becomes involved. The exact lines of responsibilities and competencies between various government agencies are also at times blurred.

The ongoing processes in Norway with respect to legislation and the associated regulations (such as the Security Act), the establishment of new institutions (such as SRMs), and new procedures and best practices (such as RHI), may mitigate some of the challenges examined in this report. In particular, the possible inclusion of some core functions of the industry under the Security Act is likely to improve security for these. However, the grey zones between the private and public sector are unlikely to disappear, and new dilemmas and challenges may emerge. The relatively high number of ministries and agencies with roles and responsibilities in the sector is a complicating factor. Until such changes are made, clearer communication channels with information between the public and private sector are required, to utilize the force, capacity and knowledge nationally. Establishing points of contact, and making sure that exchange of information between relevant actors actually takes place, are prerequisites for ensuring sufficient security; at least until a sector SRM is established. This is a government responsibility.

The Norwegian state has only a limited toolbox, and does not control most of the digital infrastructure today, which is the hands of the private sector. This impinges on the ability of the government to assist in dealing with digital incidents. Limited resources, especially in

terms of skilled cybersecurity experts, are set to remain a key challenge for Norway in the years to come. There is broad acknowledgment of the shortage of manpower and expertise in digital security, with the private sector and the public sector competing for the same scarce resource. Managing these resources, and maximizing the security that can be provided, is a daunting task that goes well beyond the petroleum sector. Creative solutions between the public and the private sector are called for, where the latter can draw on the former in case of emergency. This gives rise to a further question if both sectors are ready to cover the expenses associated with a higher level of national cybersecurity. Laws, regulations and systems are of limited value unless adequate funding is available.

Fostering cooperation between private companies and between the public and private sectors is often mentioned as a silver-bullet solution for cybersecurity. Indeed, it can serve as a vital step towards managing the pool of limited resources available, when defending against digital intrusion is of key importance (Muller 2015). However, there are no easy solutions to these issues, and building up sufficient digital security in the sector will take time.

What should be regard as 'sufficient' when it comes to cybersecurity? Thus far in the Norwegian petroleum sector, the private sector has had considerable responsibility for determining this. The new Security Act is likely to change this to some extent, with clearer regulation and legislation in the areas of the sector that are deemed to be CNI expected to be put in place. However, responsibility here also requires the ability to provide security, and repercussions in case of failure to do so. In securing the digital domain, in the petroleum sector and in general, there is still some way to go in ensuring this and the division of responsibility involved. The public sector has overall responsibility for securing CNI, but both public and private actors need to take proactive responsibility. With the exceptionally rapid evolution in digital technologies, we must recognize that legislation, regulation and organizational solutions will always lag behind. Cybersecurity is a process, not a condition.

References

Antonovich, Pavel (2011). 'Cyberwarfare: Nature and Content', *Military Thought*, 20 (3): 35–43.

Archer, Emerald M. (2014). 'Crossing the Rubicon: Understanding Cyber Terrorism in the European Context', *The European Legacy*, 19 (5): 606–621.

Atlantic Council, Digital Forensic Research Lab (2017). 'Hot Air over Natural Gas', 08.12.2017 https://medium.com/@DFRLab/balticbrief-hot-air-over-natural-gas-3679ce6bc255 accessed 15.12.2017

Bartles, Charles K. (2016). 'Getting Gerasimov Right', *Military Review*, 96 (1): 30–38.

BBC (2017a). 'UK cyber-defence chief accuses Russia of hack attacks', 15.11.2017 http://www.bbc.com/news/technology-41997262 , accessed 26.09.2017

BBC (2017b). 'Cyber-attack: US and UK blame North Korea for WannaCry', 19.12.2017. http://www.bbc.com/news/world-us-canada-42407488 , accessed 20.12.2017

Bildt, Carl (2017). 'The Pandora's Box of the Digital Age', 17 November, https://www.aspistrategist.org.au/the-pandoras-box-of-the-digital-age/

Cherepanov, Anton (2017). 'TeleBots are back: Supply-chain attacks against Ukraine', welivesecurity.com 30.06.2017. https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/, accessed 12.10.2017

Cilluffo, Frank J. (2016). 'Testimony on Emerging Cyber Threats to the United States', *U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies*, https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/HHSC_Testimony_Feb%2025-2016_Final.pdf, accessed 25.09.2017

Clapper, James R. (2016). 'Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community'. *Senate Armed*

Services Committee, 09.02.2016, https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf, accessed 25.09.2017

Connell, Michael and Sarah Vogler (2017). 'Russia's Approach to Cyber Warfare', *CNA Analysis & Solutions*, March 2017. https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf Accessed 21.10.2017

Cullen, Patrick and Erik Reichborn-Kjennerud (2016). *Countering Hybrid Warfare (CHW): Baseline assessment*, Report for Multinational Development Campaign (MCDC). Not publicly released.

Cylance Inc (2014). 'Operation Cleaver'. https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf, accessed 26.09.2017

Dagbladet (2014). 'Null CTRL' (series of articles on information security, running in early 2014, available at https://www.dagbladet.no/emne/null_ctrl)

Dagens Næringsliv (2017). 'Putin: - Norges ressurser er i ferd med å forsvinne', https://www.dn.no/nyheter/2017/06/01/1543/Energi/putin-norges-ressurser-er-i-ferd-med-a-forsvinne, accessed 25.09.2017.

The Diplomat (2015). 'Russia tops China as Principal Cyber Threat to US' https://thediplomat.com/2015/03/russia-tops-china-as-principal-cyber-threat-to-us/ accessed 26.09.2017

Dragos (2017). 'Crashoverride – Analysis of the Threat to Electrical Grid Operations' https://www.dragos.com/blog/crashoverride/CrashOverride-01.pdf, accessed 10.10.2017

ESET (2017). 'Industroyer: Biggest threat to industrial control systems since Stuxnet' https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ accessed 10.10.2017

Estonian Foreign Intelligence Service (2018) 'International Security and Estonia". https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf Accessed 05.02.2018

European Commission (2014). 'European Energy Security Strategy' http://eur-lex.europa.eu/legal-

content/EN/ALL/?uri=CELEX:52014DC0330&qid=1407855611566, accessed 21.09.2017

European Commission (2017). 'Supplier Countries' https://ec.europa.eu/energy/en/topics/imports-and-secure-supplies/supplier-countries Accessed 18.12.2017

Eurostat (2017). 'Energy production and imports' http://ec.europa.eu/eurostat/statistics-explained/index.php/Energy_production_and_imports, accessed 21.09.2017

Fardal, Harald and Ann-Kristin Elstad. 'Beslutningsprosesser i håndtering av en digital hendelse, en Garbage Can tilnærming', *Forsvarets Forskningsinstitutt,* 13.12.2017. https://www.ffi.no/no/Rapporter/17-16342.pdf Accessed 20.01.2018

FireEye (2014). 'APT28: A Window into Russia's Cyber Espionage Operations?' https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html, accessed 02.10.2017

FireEye (2016). 'Sandworm Team and the Ukrainian Power Authority Attacks', 07.01.2016. https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html, accessed 04.10.2017

FireEye (2018). 'Cyber Intelligence and Nordic Security', seminar presentation at NUPI, by Patrik Maldre, FireEye, 16.01.2018 https://www.youtube.com/watch?v=3DE8xBR8a0o

FireEye Inside Intelligence (2016) 'ICS Vulnerability trend report', p. 7. https://www2.fireeye.com/rs/848-DID-242/images/ics-vulnerability-trend-report-final.pdf Accessed 01.10.201

F-Secure (2015). 'The Dukes – 7 years of Russian cyberespionage' https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf, accessed 01.10.2017

Giles, Keir (2016), *Handbook of Russian Information Warfare*, Fellowship Monograph 9. http://fmso.leavenworth.army.mil/documents/infosecu.htm

Greenberg, Andy (2017a), 'Hackers Gain Direct access to US power grid controls', *The Wired,* 06.05.2017,

https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/ accessed 11.10.2017

Greenberg, Andy (2017b), 'The Petya plague exposes the threat of evil software updates', *The Wired*, 07.07.2017. https://www.wired.com/story/petya-plague-automatic-software-updates/ accessed 12.10.2017

Greenberg, Andy (2017c), 'The clocks read Zero when the lights went out', *The Wired*, 25.07.2017

The Grugq (2017). 'Pnyetya: Yet Another Ransomware Outbreak', 27.06.2017 https://medium.com/@thegrugq/pnyetya-yet-another-ransomware-outbreak-59afd1ee89d4 accessed 11.10.2017

Grøttan, Tor Olav. 'Angrep på Petroleumsinfrastrukturen i Norge: svakheter og konsekvenser', Presentation at NUPI 02.02.2017

Haukkala, Hiski (2015), 'From Cooperative to Contested Europe? The Conflict in Ukraine as a Culmination of a Long-Term Crisis in EU–Russia Relations', *Journal of Contemporary European Studies*, 23 (1): 25–40.

'Instruks for Etterretningstjenesten' (2001). https://lovdata.no/dokument/INS/forskrift/2001-08-31-1012

International Institute of Strategic Studies (IISS) (2013). 'The Cyber Attack on Saudi Aramco' https://www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-strategy-april-may-2013-b2cc/55-2-08-bronk-and-tikk-ringas-e272 Accessed 22.10.2017

Kaspersky Lab (2014). 'Energetic Bear – Crouching Yeti' https://securelist.com/files/2014/07/EB-YetiJuly2014-Public.pdf, accessed 01.10.2017.

Kaspersky Lab (2017). 'More than 50 percent of organizations attacked by Expetr (Petya) cryptolocker are industrial companies', 27.06.2017. https://ics-cert.kaspersky.com/alerts/2017/06/29/more-than-50-percent-of-organizations-attacked-by-expetr-petya-cryptolocker-are-industrial-companies/, accessed 12.10.2017

Kello, Lucas, (2017). *The Virtual Weapon and International Order*. New Haven, Yale University Press.

Kramer, Andrew E. (2017), 'Ukraine Cyberattack Was Meant to Paralyze, not Profit, Evidence Shows', *The New York Times*, 20.06.2017. https://www.nytimes.com/2017/06/28/world/europe/ukraine-ransomware-cyberbomb-accountants-russia.html, accessed 11.10.2017

Lunde, Morten Haga (2017). 'Fokus - NIS assessment of current security challenges', Speech at *Sårbarhetskonferansen 2017,* Oslo, 26 September.

Matthews, Owen (2015). 'Russia's Greatest Weapon may be its Hackers', *Newsweek,* 15.05 2015. http://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its- hackers-328864.html. accessed 26.08.2017

Maurer, Tim (2015). 'Cyber Proxies and the Crisis in the Ukraine', in Kenneth Geers (ed.) *Cyber War in Perspective: Russian Aggressions against Ukraine,* NATO CCD COE Publications, Tallinn.

Meld. St. 29 (2011-2012): 'Samfunnssikkerhet'. https://www.regjeringen.no/no/dokumenter/meld-st-29-20112012/id685578/

Meld. St. 10 (2016-2017): 'Risiko i et trygt samfunn – samfunnssikkerhet'. https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20162017/id2523238/

Meld. St. 38 (2016-2017), 'IKT-sikkerhet, et felles ansvar'. https://www.regjeringen.no/no/dokumenter/meld.-st.-38-20162017/id2555996/

Ministry of Justice and Public Security (2012). 'Nasjonal strategi for Informasjonssikkerhet: Handlingsplan'. https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-informasjonssikker/id710469/ Accessed 29.01.2018

Muller, Lilly Pijnenburg (2015). 'Securing Cyberspace. Coordinating Public-Private Cooperation'. NUPI Policy Brief 20.

Munson, Lee (2014). 'Massive cyber attack on oil and energy industry in Norway' *Naked Security* 28.08.2014. https://nakedsecurity.sophos.com/2014/08/28/massive-cyber-attack-on-oil-and-energy-industry-in-norway/ accessed 20.09.2017

Nasjonal Sikkerhetsmyndighet (2014) 'Varslingssystem for digital infrastruktur (VDI)'. https://nsm.stat.no/norcert/varslingssystem-for-digital-infrastruktur-vdi/ Accessed 20.12.2017

Nasjonal Sikkerhetsmyndighet (2017). 'Helhetlig IKT-risikobilde 2017'. https://www.nsm.stat.no/globalassets/helhetlig_ikt-risikobilde_2017_orig_low.pdf

Nasjonal Sikkerhetsmyndighet (forthcoming 2018). *Framework for Management of Digital Incidents / Rammeverk for håndtering av IKT-sikkerhetshendelser*.

National Cybersecurity and Communications Integration Center (USA) (2017). 'Destructive Malware' (White paper) https://ics-cert.us-cert.gov/sites/default/files/documents/Destructive_Malware_White_Paper_S508C.pdf accessed 11.10.2017

Norsk Petroleum (2017). 'Eksport av Olje og Gass' http://www.norskpetroleum.no/produksjon-og-eksport/eksport-av-olje-og-gass/ Accessed 18.11.2017

The Norwegian Intelligence Service (NIS) (2017). 'Fokus, NIS assessment of current security challenges' https://forsvaret.no/en/ForsvaretDocuments/Fokus2017_2002_ENGELSK_v2.pdf accessed 24.10.2017

NOU 2015:13 'Digital sårbarhet – sikkert samfunn: Beskytte enkeltmennesker og samfunn i en digitalisert verden' (Lysne I) https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf.

Nougayrede, Natalie (2017). 'As the US and the EU square off over Russia sanctions, only Putin can win', *The Guardian,* 31.07.2017 https://www.theguardian.com/commentisfree/2017/jul/31/europe-us-russia-sanctions-putin-washington-eu-donald-trump accessed 15.12.17

Olsen, Øystein (2015). 'Oljen og Norsk Økonomi', lecture 14.10.2015. http://docplayer.me/25134528-Oljen-og-norsk-okonomi-sentralbanksjef-oystein-olsen-ntnu-29-september-2015.html accessed 21.09.2017

Orttung, Robert W. and Indra Øverland (2011). 'A limited toolbox: Explaining the constraints on Russia's foreign energy policy', *Journal of Eurasian Studies,* 2 (1): 74–85

Petroleum Act (1996). https://lovdata.no/dokument/NL/lov/1996-11-29-72 Accessed 10.01.2018

Petroleum Safety Authority (PSA) (2017a). 'Brief: IKT-sikkerhet: Tilsyn med operatører og redere' at NUPI 2017

Petroleum Safety Authority (PSA) (2017b), "Security and Responsibility", http://www.ptil.no/sikkerhet-status-og-signaler/ny-publikasjon-sikkerhet-og-ansvar-article13353-820.html accessed 22.01.2018 accessed 22.01.2018

Petroleum Safety Authority (PSA) (2017c), 'Guidelines Regarding the Facilities Regulation', 18.12.2017. http://www.ptil.no/facilities/category405.html accessed 22.01.2018

Petroleum Safety Authority (PSA) (2017d), 'Regulations relating to design and outfitting of facilities, etc. in the petroleum activities (The Facilities Regulations)', 18.12.2017. http://www.ptil.no/facilities/category400.html Accessed 22.01.2018

Petroleum Safety Authority (PSA) (2017e), 'Regulations relating to management and the duty to provide information in the petroleum activities and at certain onshore facilities (The Management Regulations)', 18.12.2017. http://www.ptil.no/management/category401.html accessed 22.01.2018

Petroleum Safety Authority (PSA) (2017f), 'Regulations relating to health, safety and the environment in the petroleum activities at certain onshore facilities (The Framework Regulations). 15.12.2017. http://www.ptil.no/framework-hse/category403.html Accessed 22.01.2018

Police Act (1995). Accessible at https://lovdata.no/dokument/NL/lov/1995-08-04-53

Police Security Service (PST) (2017). 'Trusselvurdering 2017', 10.10.2017. https://www.pst.no/trusselvurdering-2017/ accessed 24.10.2017

Police Security Service (PST) (2018). 'Trusselvurdering 2018', 30.01.2018 https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2018/ accessed 08.02.2018

Prop. 151 S (2015–2016), 'Kampkraft og bærekraft, Langtidsplan for forsvarssektoren'. https://www.regjeringen.no/no/dokumenter/prop.-151-s-20152016/id2504884/sec1

Prop 153L (2016-2017), 'Lov om nasjonal sikkerhet (sikkerhetsloven). https://www.regjeringen.no/no/dokumenter/prop.-153-l-2016-2017/id2556988/sec1

Reuters (2017). 'Cyber 'Worm' Attack Hits Global Corporate Earnings'. http://fortune.com/2017/08/02/cyber-worm-attack-corporate-earnings/ Accessed 12.12.2017

Rid, Thomas and Peter McBurney (2012). 'Cyber Weapons', *The RUSI Journal*, 157 (1): 6–13

Riley, Michael, Jordan Robertson and Anita Sharpe (2017). 'The Equifax hack has the Hallmarks of State-Sponsored Pros', *Bloomberg Businessweek*, 29.09.2017. https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros , accessed 11.11.17

Rogers, Michael S. (2016). 'Statement made to House Armed Service Committee' in March 2016, transcript available at http://docs.house.gov/meetings/AS/AS26/20160316/104553/HHRG-114-AS26-Wstate-RogersM-20160316.pdf accessed 15.09.2017

Schia, Niels Nagelhus (2017). 'The Cyber Frontier and digital pitfalls in the Global South". Third World Quarterly. Published online end accessible at http://www.tandfonline.com/doi/full/10.1080/01436597.2017.1408403

Shane, Scott, Nicole Perlroth and David E. Sanger (2017). 'Security Breach and Spilled Secrets Have shaken the NSA to Its Core', *New York Times* 12.11.2017. https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html accessed 13.11.2017

Symantec (2014). 'Emerging Threat: Dragonfly/Energetic Bear – APT group', 30.06.2014. https://www.symantec.com/connect/blogs/emerging-threat-dragonfly-energetic-bear-apt-group accessed 02.10.2017

Symantec (2017a). 'What you need to know about the Wannacry Ransomware', 23.05.2017. https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware accessed 26.09.2017

Symantec (2017b), 'Dragonfly: Western energy sector targeted by sophisticated attack group'. 20.10.2017

https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group Accessed 24.10.2017

Trend Micro (2016). 'Security Predictions, The Next Tier' https://www.trendmicro.com/vinfo/no/security/research-and-analysis/predictions/2017 Accessed 22.11.2017

Utenriksdepartementet (2017), 'Internasjonal cyberstrategi for Norge', https://www.regjeringen.no/globalassets/departementene/ud/dokumenter/sikpol/cyberstrategi_web.pdf%20

Verdens Gang (2017a) , 'Ni norske epostkontoer utsatt for målrettet russisk hackerangrep, også PST selv' 03.02.2017 https://www.vg.no/nyheter/innenriks/politiets-sikkerhetstjeneste-pst/pst-ni-norske-epostkontoer-utsatt-for-maalrettet-russisk-hackerangrep-ogsaa-pst-selv/a/23915390/ accessed 25.09.2017

Verdens Gang (2017b), 'Russland hardt ut mot Norge: Ikke holdbart', 17.02.2017 https://www.vg.no/nyheter/innenriks/russland-hardt-ut-mot-norge-ikke-holdbart/a/23927882/ accessed 22.09.2017

Zetter, Kim (2016)., 'Evidence suggests the Sony Hackers are alive and well, still hacking', *The Wired* 12.02.2016. https://www.wired.com/2016/02/evidence-suggests-the-sony-hackers-are-alive-and-well-and-still-hacking/ accessed 09.10.17

Norwegian Institute of International Affairs

Established in 1959, the Norwegian Institute of International Affairs [NUPI] is a leading independent research institute on international politics and areas of relevance to Norwegian foreign policy. Formally under the Ministry of Education and Research, NUPI nevertheless operates as an independent, non-political instance in all its professional activities. Research undertaken at NUPI ranges from short-term applied research to more long-term basic research.

About the Authors:

Lilly Pijnenburg Muller is a Research Fellow in the Research Group for Security and defenceat the Norwegian Institute of International Affairs (NUPI) with a focus on cybersecurity. Within cybersecurity her research covers public-private cooperation, multi-stakeholder processes, capacity building in developing countries, risk and harm. In addition, she follows international cybersecurity processes in the UN, OSCE and NATO.Previously she worked as a James Martin Fellow at the University of Oxford at the Martin Schools Global Cyber Security Capacity Building Center (GCSCC).

Karsten Friis is a Senior Adviser and head of NUPIs Research Group on Security and Defence. His main area of expertise is security and defense policies, international military operations, civilian-military relations, cyber security, as well as the political developments in the Western Balkans. Friis has previously worked for the Organization for Security and Cooperation in Europe (OSCE) in Serbia, Montenegro and Kosovo, as well as for the Norwegian Armed Forces in Oslo and in Kosovo. He holds a Cand. Polit. in Political Science from the University of Oslo and a MSc in International Relations from London School of Economics.

Lars Gjesvik works as a research assistant at the Research group for Security and Defence. His research primarily focuses on different dimensions of cybersecurity, with previous publications centering around issues of cybersecurity in developing countries and cyber sovereignty. He is currently a masters student at the University of Oslo, writing his masters thesis on the security challenges facing digital energy systems.

NUPI
Norwegian Institute of International Affairs
C.J. Hambros plass 2D
PO Box 8159 Dep. NO-0033 Oslo, Norway
www.nupi.no | info@nupi.no