RESEARCH AND ANALYSIS

Research Report

Nuclear energy and the current security environment in the era of hybrid threats

Research Report

Nuclear energy and the current security environment in the era of hybrid threats

Hybrid CoE Research Reports are thorough, in-depth studies commissioned by Hybrid CoE, or products of joint Hybrid CoE projects. These reports aim to provide a comprehensive understanding of issues relevant to hybrid threats. They either provide relevant policy recommendations or other practical conclusions, and include new research with relevant references. Hybrid CoE provides feedback on the reports before their publication.

The European Centre of Excellence for Countering Hybrid Threats tel. +358 400 253800 www.hybridcoe.fi

ISBN 978-952-7282-24-3
October 2019

Hybrid CoE is an international hub for practitioners and experts, building member states' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats located in Helsinki, Finland.

Preface

With the rising prominence and increased understanding of hybrid threats, it can be foreseen that those seeking to challenge democratic states will look for new ways to deploy national power to further their own strategic interests. Could nuclear energy be used as one of the strategic tools in hybrid threat activity for geopolitical aims? As this question has received insufficient attention to date, the aim of this research paper is to generate discussion on the subject and take it forward.

This report is a joint effort by four Centres of Excellence around the Baltic Sea, each of which have their own focus and niche. The initiative for the report stemmed from the Lithuanian Ministry of Foreign Affairs and was endorsed by the directors of the European Centre of Excellence for Countering Hybrid Threats, the NATO Energy Security Centre of Excellence, the NATO Cooperative Cyber Defence Centre of Excellence, and the NATO Strategic Communications Centre of Excellence.

The report includes three case studies: Ostrovets nuclear power plant (NPP) in Belarus, the Paks NPP project in Hungary, and the Hanhikivi NPP project in Finland. The case studies also revealed that the Russian state nuclear energy company Rosatom should be examined as a significant actor in the European nuclear energy sector due to the fact that it also has ambitions outside of Europe. These projects in Europe are examples of such strategic ambitions of the company.

The NATO accredited Energy Security Centre of Excellence (ENSEC COE) in Vilnius, established in 2012, pushed the Lithuanian MFA's initiative forward with the Ostrovets case study, as well as its expertise in energy matters. ENSEC's mission is to assist Strategic Commands, other NATO bodies, nations, partners, and other civil and military entities by supporting NATO's capability development process, mission effectiveness, and interoperability in the near-, mid- and long-term by providing comprehensive and timely subject matter expertise on all aspects of energy security. The mission includes cost-effective solutions to support military requirements, energy efficiency in the operational field, and interaction with academia and industry (ENSEC COE, 2019).

Insights into the cyber field were provided by the NATO accredited Cooperative Cyber Defence Centre of Excellence (CCDCOE), established in 2008. NATO CCDCOE is a cyber defence hub focusing on research, training and exercises. The international military organisation based in Estonia is a community of 25 nations providing a 360-degree view of cyber defence, with expertise in the areas of technology, strategy, operations and law. The CCDCOE is known for its *Tallinn Manual*, the main source of reference for international law applicable to cyber operations. CCDCOE's mission is to support its member nations and NATO with unique interdisciplinary expertise in cyber defence (CCDCOE, 2019).

The NATO-accredited Strategic Communications Centre of Excellence (StratCom COE) in Riga, established in 2014, analysed the dynamics of information influence activity that surround nuclear energy and the different levers of persuasion and coercion available to an adversary. The Centre's mission is to provide a tangible contribution to the strategic communications capabilities of NATO, NATO allies and NATO partners. Its strength is built by multinational and cross-sector participants from the civilian and military, private and academic sectors, and the usage of modern technologies, virtual tools for analyses, research and decision-making (StratCom COE, 2019).

The project has been led by the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), established in Helsinki in 2017. Hybrid CoE currently embraces 24 member states as well as the EU and NATO. Hybrid CoE's unique networked-based working model aims to assist member states and institutions in understanding, deterring and countering hybrid threats and in capability- and resilience-building, as well as by serving as a safe place where best practice, lessons

identified and new ideas can be shared. Hybrid CoE acted as the editor-in-chief of the report, contributed its knowledge of the Hybrid Threats Conceptual Model, including different phases of hybrid activity, and integrated these into the case studies, as well as contributed two case studies (Hybrid CoE, 2019).

We would like to extend special thanks to Mr James Henderson from the Oxford Institute for Energy Studies for setting the scene and providing a global perspective on the activities and motives of Rosatom. When analysing hybrid threat potential, context and empirical evidence are central to being able to analyse what is an immediate threat, what is a potential future threat, and what might look like a threat but is not.

This report does not claim to be a comprehensive study of nuclear energy and how it can be used as one of the tools in coordinated and synchronised action in the landscape of hybrid threats. It is an initial study upon which future risk assessments and scenario-based exercises relating to nuclear energy can build.

This process would not have been possible without the cooperation between the Centres of Excellence and their shared understanding of the contemporary security environment.

Table of Contents

Introduction

Security concerns are an integral part of the discussions on energy dependencies. The security discussion became even more common in the European energy debates with the various gas disputes between Russia and Ukraine in 2006–2015. After these incidents, the energy diversification policy has received increasing attention in Europe. Russia has featured prominently in the European debate relating to energy dependencies and interdependencies, but there are also other actors who may have an interest in affecting the stability of the energy supply. This has been the case with hydrocarbon production and exports in particular (Oxenstierna, 2014). Recent attacks on oil tankers and an oil processing facility in Saudi Arabia have made headlines and resulted in rapid fluctuations in the price of oil. Nuclear energy has attracted much less attention as a potential security risk compared to the perception of risks related to hydrocarbon dependency, and it is therefore worth taking a closer look at the sector.

Different energy sources, industries and actors must be studied more carefully in the changed security environment. These changes include the growing dependencies across energy infrastructure systems, increasing interconnectedness in the world, the increased potential to use energy as a geo-political tool and the intensifying competition among great powers and regional hegemons (Verner, et al., 2019). The objective of this study is to analyse whether nuclear energy can be used in some way by an adversary as a part of their hybrid activity toolbox.

The first part of the report will contextualise the way in which we should conceptualise hybrid threats, and illustrate how any adversary might put together a toolbox to make an intervention in any state's sovereign space, in order to further their own strategic interests. To this end, the report will apply the conceptual model developed in the joint report by Hybrid CoE and the European Commission Joint Research Centre (JRC), 'The Landscape of Hybrid Threats – A Conceptual Model'. According to the Hybrid CoE-JRC report, an adversary might employ highly creative combinations of different tools in multiple domains in order to achieve its targets and strategic goals. Hence, every subject studied through the hybrid threat lens should include different disciplines. The Hybrid CoE-JRC conceptual model includes 13 domains and three phases of activity. The domains most relevant to nuclear energy – infrastructure, cyber, economy and information, as well as all three phases – are analysed in this study. The hybrid threat analysis also requires viewing the role of nuclear energy in a political and geographical context. It is not only important to consider the role of nuclear energy in the national and regional (European) energy mix and energy markets, but also to consider potential threats relating to nuclear energy outside European markets.

The first chapter of the second part of the report, written by James Henderson, will examine different empirical cases. It starts by looking at Rosatom as an actor. Russia is the most important foreign actor in the EU in the energy sector and it has an established position in the European nuclear energy markets. As the European Commission states, "Russia is a key competitor in nuclear fuel production and offers integrated packages for investments in the whole nuclear chain. Therefore, particular attention should be paid to investments in new nuclear power plants to be built in the EU using non-EU technology, to ensure that these plants are not dependent only on Russia for the supply of the nuclear fuel: the possibility of fuel supply diversification needs to be a condition for any new investment, to be ensured by the Euratom Supply Agency" (European Commission, 2014). On the Russian side, Rosatom is a state corporation and belongs to the strategic sector in which the Russian state is heavily involved. In recent years, Rosatom has established itself as an important player in international markets.

After discussing Rosatom's role and position in the European nuclear energy markets, the report

continues with three case studies of NPPs in three European states: Ostrovets in Belarus, Hanhikivi in Finland and Paks in Hungary. It is through these case studies that we learn how different processes can create potential hybrid threats, and how business deals and actions sometimes have their respective challenges and competitions, but that not everything will become a security threat.

The case studies have been chosen on the basis that all of them have in their own way an important place in European energy security, and all of them have Russian-designed reactors. Ostrovets in Belarus is not inside the EU and Belarus is not a NATO member. However, as the Chernobyl experience from the 1980s has shown, a nuclear power plant accident will not only be a matter for the country that hosts the NPP. The consequences of an accident are wider and also affect neighbouring states.

The Paks NPP development in Hungary is clearly in line with the Hungarian energy strategy. Any connection to threats is hard to detect, at least at first glance. However, the Paks development did require the European Commission's intervention and the role of Rosatom is central in this respect. Lack of transparency in the process has duly raised concerns.

In the case of Hanhikivi in Finland, a certain continuity can be detected in the Finnish energy policy. However, the public debates relating to the project justify looking at the project development from the hybrid threat perspective as well. Even if the business deal can be seen as business as usual, such a deal may expose a vulnerability for the host state.

The report will conclude that nuclear energy and nuclear power plants – as part of the hybrid threat landscape – are indeed an area that needs to receive more attention in the current security environment. An ordinary-looking business deal may have threat potential embedded in it and the capacity to destabilise a state. Nuclear energy might not reflect the same kind of vulnerability as physical connections or logistical dependency, such as pipelines or dependency on sea lanes. However, nuclear energy is much more connected to created threat perceptions, diverting a business culture away from host countries' preferences, as well as creating financial dependencies.

PART I:
Hybrid threats as a part of today's security environment

The changes in our security environment during recent years have brought to the surface discussions relating to hybrid threats. Hybrid threats characterise the changing nature of security and they include both objective and subjective threats. Objective threats can be measured against external criteria and the subjective dimension can be defined as the individual perception of being safe (Johansson, 2013). In fact, one of the specificities relating to hybrid threats is that they are very much based on subjective threats to blur situational awareness and confuse any decision-making. The aim is to lure the target to make mistakes and decisions that inflict self-harm.

Although very difficult to define, hybrid threats can be characterised as coordinated and synchronised action that deliberately targets the systemic vulnerabilities of democratic states and institutions through a wide range of means. These activities exploit the thresholds of detection and attribution, as well as different borders between war and peace, internal and external, local and state, friend and enemy, and so forth. The aim of this type of activity is to influence different forms of decision-making at the local (regional), state, or institutional levels, in order to favour and/or further the adversary's strategic goals while undermining and/or hurting the target (Hybrid CoE, 2019).

Hybrid threats may entail many types of activity, including interference (leverage-building, vulnerability identification and penetration into the target country), influencing (using the established leverage and detected vulnerabilities), operations and campaigns (both interference and influence are used and activity of a more damaging nature), and even warfare (where the use of military force is included in the activity).

It must also be kept in mind that it is often difficult to assess who is behind the hybrid threat activities and what the level of the actual threat is. It is important to understand that hybrid threat-related activity is always tailor-made and target-specific.

Hybrid threat domains[1]

Activities pertaining to the landscape of hybrid threats can occur in multiple domains and exploit multiple tools. The report by Hybrid CoE and the EU Joint Research Centre identifies 13 different domains: economic, military, legal, cultural, social, diplomacy, infrastructure, information, cyber, space, political, administration and intelligence. Naturally, an adversary might find new domains, since the nature of hybrid threats is highly creative and ever-changing. However, these 13 domains provide an expanded picture of what can be obtained with traditional vulnerability analyses such as DIMEFIL[2] or PMESII.[3]

In the infrastructure domain, nuclear energy and nuclear power plants are often examined from the security of supply perspective. **In the hybrid threat context,** nuclear energy should not only be looked at from the security of supply perspective, but should also include economic leverage-building (including interference in internal energy markets), nuclear proliferation and terrorism, cyber threats and information influencing activities.

Part of the hybrid threat analysis entails considering the different degrees of activity intensity. This is viewed through the three phases of hybrid activity: **priming**, **destabilisation** and **coercion**. It must also be kept in mind that it is often difficult to assess who is behind the hybrid threat activities and what the actual threat level is. Likewise, it is

1 The following section is based on the report by Hybrid CoE & JRC entitled *The Landscape of Hybrid Threats: A Conceptual Model* (2019) (forthcoming).
2 Diplomatic, Information, Military, Economic, Financial, Intelligence and Law Enforcement.
3 Political, Military, Economic, Social, Information, Infrastructure.

important to understand that **hybrid threatrelated activity is always tailor-made and targetspecific.**

Phases of hybrid activity

In some cases, the activity in the three aforementioned phases – priming, destabilisation and coercion – overlaps and there is the potential for escalation, although this is not always the case. De-escalation may also occur, meaning that the activity may backtrack, confusing situational awareness and disguising the real aims of the action. This is an important characteristic of hybrid threats. It also means that different types of threshold manipulation become possible.[4]

Priming

In the psychological literature, priming is action that aims to facilitate change in an organisation or an environment (Oyserman & Lee, 2008; Molden, 2014). The idea behind priming is that it seeks to bring about a long-term effect in the attitude or behaviour of an individual, group or organisation. The priming technique facilitates testing cultural factors by clarifying what is salient and accessible to the participants at the point when a judgement is made or behaviour engaged in. When applying the concept of priming to threat and risk assessments, we see a long-term process of building leverage, learning and testing through interference. The priming activities can be seen as completely legal, only creating a potential threat while testing the borders between acceptable and unacceptable, as well as legal and illegal.

A good example of priming is the way in which information has been used. It has been shown that in conducting information activities, the aggressor studies a society, including the social cleavages, controversies and problems, and attempts to exploit the tensions therein by using illegitimate methods (Pamment, et al., 2018, p. 21). Priming can also target individuals or different types of communities, especially those that feel marginalised by their state. Such priming activities may include lobbying for favourable media reporting, social media adverts, participating in social media discussions, inserting a particular narrative into news and reporting, and so on. This differs from outright lies and propaganda, which belong to the destabilisation phase, by being a more subtle action and exploiting the freedom of speech principle.

Another often-mentioned area for priming is cyber. Activities in cyberspace can cause damage to critical infrastructure. Different types of disruption and overloading operational systems via cyber means are part of the toolkit. Cyber activities may be used for information gathering, for example by hacking and reconnaissance. In the cyber domain, it is easier for the adversary to remain anonymous, which makes it a suitable platform for hybrid activity, as attribution becomes difficult and ambiguity increases. The priming phase entails interference and some disturbances, but stops short at disruptions and actions that cause physical damage.

Priming in the economic domain includes activities like building leverage through economic means. This has long roots when seeking ways to exert influence: conditionality relating to loans, foreign direct investment (FDI), ownership relating to property or business, and so forth (Mattlin & Nojonen, 2011). All of the case studies in this report show that the economic domain has been an important part of leverage-building when it comes to nuclear energy.

The logic of priming relating to hybrid threats differs from preparing for an open conflict: priming is a long-term activity – it is carried out in anticipation, rather than in a clear, goal-oriented way, and the activity is often legal and in some ways overt, if you know where to look. However, the aims and reasons behind the action are blurred. Sometimes the real adversary behind the action also fades into the background, and if the same actor is active in several different domains, attribution is virtually impossible. Even if activity can be detected, connecting it to an adversary is very difficult. The same actor may be active in several different domains, but in such a way that making a connection between diverse activities in various domains can be extremely hard.

Destabilisation

Destabilisation activity exploits the different grey zones between areas that are traditionally seen as separate, but which in today's security environment are closely interlinked and intertwined, like

4 *The Landscape of Hybrid Threats: A Conceptual Model* (2019), Hybrid CoE & JRC (forthcoming).

external and internal security; state- and local-level connections; perceptions relating to friend and foe; areas pertaining to different authorities' jurisdictions and different legal frameworks; and even understandings relating to war and peace.

One of the aims of exploitation of these interfaces is the dissolution of fixed categories of order. The resulting ambiguity prevents, paralyses or impedes a fast, unified response either from the target or the international community. As in the priming phase, the real actor behind an event might be unknown. Even if the actor is clearly known, attribution is still difficult.[5]

The destabilisation phase includes the use of influence in an operative manner, and the activity of the adversary is synchronised and coordinated. The activity becomes hybrid in that more than one tool is used and it has a strategic aim. During the destabilisation phase, the actor might aim for a long campaign (multiple operations in different domains) or use the opportunity for one operation and then de-escalate and return to the priming phase.

For instance, if Russia intended to stop the desynchronisation of the Baltic electricity grids from the Russian IPS/UPS synchronous area in order to ensure a future market for the Ostrovets NPP output, Russia could launch multiple operations in different domains with different degrees of intensity. These measures could include acts such as corrupting officials at the decision-making level (administration/intelligence domains), causing disturbances in the desynchronisation exercises (cyber domain), lowering the price of the electricity from Ostrovets NPP (economic domain) and establishing a social media campaign to support claims for the need for cheaper electricity (information domain).

A typical feature of hybrid threat activity is to conduct the activity in a domain or geographical location that is not the primary target. In this way, attention is diverted to the wrong place. If the desired effects are not achieved, the activity either returns to priming and starts a new tailoring process to make a new, improved combination or create new vulnerabilities, or escalation is bound to occur. This depends on several issues, namely the importance of strategic goals, responses and opportunities.

Coercion

During the coercion phase, the activity can be termed hybrid warfare or hybrid war. When the activity has become detectable and attributable, the term hybrid warfare is appropriate. The activity in this phase represents the "hard end" of the escalation spectrum of hybrid threats. While it potentially makes use of all strategic domains and sources of power, hybrid warfare includes the use of force as its defining element. From terror, sabotage and subversion to guerrilla-warfare, conventional warfare and even the nuclear energy domain, all possible levels of escalation can be included and combined (Schmid, 2019).

Coercion activities could include causing physical damage that would have serious implications for the whole society, for instance. This could take the form of a cyber attack or even a terrorist operation that would cause a leak of radioactive material, result in civilian casualties, and test the response from the authorities, the EU and NATO. Another example would be radioactive material getting into the hands of hostile non-state actors, either by accident or by design, which could cause cascading effects in other domains. Combined with a heavy information campaign, such an incident could lead to public panic, which in itself would duly cause disruptions to state functioning.

As the MCDC project has concluded, there is a continuum of competition and conflict where hybrid warfare takes place. Hence, the challenge is not just to form and understand a unified concept of hybrid threats, but also to form policies and strategies that take into account the location of the threat in this continuum. Actions taken to counter hybrid warfare must consider the nature, type and degree of the threat. (MCDC, 2019)

This chapter has discussed the degrees of hybrid threats. In the following section, nuclear energy is studied from the perspective of its (potential) type and nature. The question of how nuclear energy and nuclear power plants are related to hybrid threats is discussed under the topics of security of supply, economic leverage, cyber security and information influencing.

5 *The Landscape of Hybrid Threats: A Conceptual Model* (2019), Hybrid CoE & JRC (forthcoming).

Potential security threats related to nuclear energy

Energy is related to security aspects in many ways. The concept of energy security is used in policy texts in particular as a synonym for security of supply, but it has also been used in the sense of an important contributor to conflicts and other security threats (Johansson, 2013). Energy security has been examined from at least three different perspectives: physical security (supply security), price security (economic aspects) and geopolitical security (UK Energy Research Centre, 2009). This report focuses on nuclear energy and investigates whether it has been overlooked when analysing security threats relating to energy, especially in the era of hybrid threats. Firstly, the security of supply aspect is examined, followed by an analysis of the economic domain and leverage-building. Nuclear proliferation, terrorism and the cyber domain are subsequently studied in the context of nuclear energy, and the section concludes with an examination of the information domain.

Security of supply

At first glance, an NPP is quite similar to any fossil fuel power plant. Nuclear power is a cheap and reliable source of energy that provides the base-load supply of electricity. It produces greenhouse gas emissions and air pollution comparable to any renewable energy source – virtually none during production, and very low emissions over its life cycle. As of August 2019, there were 451 nuclear power reactors in operation and 54 under construction worldwide (IAEA, 2019). Nuclear power provides approximately 11% of global electricity and avoids 2 billion tonnes of GHG equivalent emissions (IAEA, 2017).

In the EU, 14% of the whole electricity consumption and 27% of electricity generation is powered by nuclear energy. There are 131 nuclear power plants in 16 member states, the majority of which are in France, Germany, the UK, Spain and Sweden. In 1957, the Euratom Treaty unified the process of managing nuclear energy production in its signature countries, and set up the Euratom Supply Agency in order to safeguard the supplies and equal access of all EU users to sources of supply. (European Commission, 2014; WNA, 2018)

The way in which the European Commission writes about nuclear energy is still in terms of the supply security of uranium. 95% of the uranium is imported from various supplier countries, such as Kazakhstan, Canada and Russia. In this area, there is vulnerability due to dependency on Russian uranium-processing services (such as final fuel assembly) for Russian-designed reactors. In the EU, there are two types of reactors: Western-designed and Russian-designed. According to the Commission, the Western-designed reactors have a more diversified process compared to the Russian-designed reactors, where the process is managed by one Russian company, TVEL, currently with insufficient competition, diversification of supplier or back-up. As a result, EU fuel assemblies are approximately 40% dependent on processes managed by external suppliers. The Russian-designed reactors are located in Bulgaria, the Czech Republic, Finland, Hungary and Slovakia. (European Commission, 2014)

Nuclear energy might not be as time-sensitive to disruptions as oil and gas. For example, the Finnish company Fennovoima has estimated that nuclear power plants usually hold fuel storage equivalent to one year of operation. Fuel rods can also be stocked for longer periods of time for security of supply purposes (Fennovoima, 2014, p. 61). In addition, there are several proposals for multilateral approaches in the global nuclear industry that focus on supplementary mechanisms of supplying nuclear fuel in case of bilateral political disagreements between an enricher and a customer state (WNA, 2011).

There could be many reasons for possible interruptions to security of supply in the field of nuclear

energy. The EU considers that possible interruptions to the supply of uranium might be caused not only by the nuclear industry's development, such as domestic needs of the supplier, but also by political disturbances: "Reasons can be manifold and may be factual such as preferential supply of domestic needs in case of scarce resources, avoidance of excessive dependency on a single supply source, protection of domestic nuclear industry, anti-dumping actions or sustainability issues. Restrictions, however, may also be driven by reasons that are completely outside the nuclear industry's sphere such as trade conflicts or political disturbances between nations or regions" (Euratom Supply Agency, 2015).

The economic domain – leverage-building

New aspects of threats in the hybrid threat landscape include the way in which business deals can have a potential threat embedded into them. Business agreements have not usually been viewed as a security issue, but in today's security environment this is a growing trend that warrants further analysis. The IAEA has noted that "in many cases, the goals of government-to-government financing go beyond the specific project and include establishing long-term bilateral relationships. The nature of this relationship may ultimately determine the conditions and repayment of the government-to-government loans" (IAEA, 2018).

The concerns relate in particular to the Russian and, to some extent, Chinese way of engaging in foreign direct investment in infrastructure projects. For example, an agreement with any actor to build a nuclear power plant typically comes with a package of long-term contracts to operate, maintain, and even refuel the plant. These agreements can also include regulatory consulting, which allows a foreign state to help shape the laws governing strategic sectors. For example, in the case of Turkey's Akkuyu NPP, Rosatom has proposed a Build-Own-Operate (BOO) model, which according to the AC report would make Turkey "the first in the world to rely on a foreign vendor to own and operate a nuclear power plant in its country" (Stein, 2016). As Rosatom's Director General Alexey Likhachev put it, "What makes this project unique is the Build-Own-Operate approach. This is the world's first nuclear project in which our company is responsible for every stage of the plant's life, from design and construction to operation and decommissioning. For this reason, the project is viewed as a strategic investment" (Rosatom, 2019). After such a plant becomes operational, the host country has limited oversight in terms of what is happening in the territory around the plant. Potentially, it could be used to support intelligence and special operations in the region. This leverage may decline over time, as the host country trains more technical specialists (Hillman, 2019).

The conditionality that applies to loans and sometimes to foreign direct investments is, to some extent, imposed by all. The traditionally cherished and widely accepted view is that the Chinese practice of providing aid primarily in the form of turnkey[6] projects that require intensive Chinese involvement in all project phases, including post-construction management during handover, does not constitute interference in the recipient countries' domestic affairs; it merely teaches recipient countries to become self-reliant. However, as Mikael Mattlin and Matti Nojonen argue, this is only true in a narrow sense. In the broader sense, strings such as political and embedded conditionality are attached (Mattlin & Nojonen, 2011).

It is possible that government-to-government business deals will end up profiting all sides. However, in the era of hybrid threats and renewed contestation among great powers, one must take a traditional geopolitical reading into account. There is a possibility that non-democratic countries will use conditionality to their advantage, especially in order to try to suppress any criticism that might emerge from democratic countries relating to the domestic affairs of authoritarian states or the investment and lending provided by them.

Nuclear proliferation and terrorism

The technologies and materials required to produce nuclear energy have a dual-use capability. This means that any nuclear activity declared by states as peaceful could be used to advance

6 Under a turnkey contract, a firm agrees to fully design, construct and equip a manufacturing facility and turn the project over to the purchaser when it is ready for operation for a fee.

capabilities to build nuclear weapons. The technological path is not straightforward, and all countries that have signed the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) accept the obligation to allow IAEA inspectors into their nuclear energy facilities in order to reduce the danger that governments might cheat on their commitments not to use the technology to acquire nuclear weapons. (Miller & Sagan, 2009) However, despite the fact that this process is contained in peacetime and especially on behalf of democratic states, controversies remain relating to nuclear energy that stem from radioactivity of the fission process and nuclear fuel throughout its life cycle.

It is fair to point out that all illegal/unlawful nuclear weapons programmes, whether known or strongly suspected, have been undertaken by non-democratic governments (Miller & Sagan, 2009). The problems that may follow have made headlines in recent decades especially in relation to the Democratic Republic of North Korea and the Islamic Republic of Iran. In this way, nuclear proliferation can also be a part of political warfare and therefore conflict proneness is a part of the picture and also directly related to geopolitical security.

A vulnerability that should be considered, especially if corruption is high in the country in question, is the presence of an insider who is privy to information and who has access to the control systems. Insiders could be hard to detect and would be able to inflict much harm, either in the form of physical damage or intelligence gathering. Threats relating to a corrupt insider are usually managed through routines: security clearance, limited access and by analysing log files for suspicious activities, and so forth. This reduces the insider risk, but will not remove it altogether. The companies maintaining the facility also have access to the control systems and their personnel should therefore be included in all security routines or even work under surveillance. The same goes for the supply chain; when old equipment is replaced, it is essential to retain control over it to ensure that there are no preinstalled vulnerabilities in the new equipment.

Furthermore, insiders might not always know that they are being used by an outsider to cause harm. For instance, in the case of the Stuxnet attack on Iran nuclear centrifuges, the creators of the malware inserted it into the internal, air-gapped network of the nuclear reactor facilities by infecting the computers of companies working with a service provider, whose computer systems were used at the facilities to monitor the uranium enrichment process. In this way, the companies working with the service provider were used as insiders and were oblivious to the fact that they were malware "carriers". Once the computers were infected, the malware spread via USB flash drives (Zetter, 2014).

Theoretically, the threat from nuclear terrorism covers a broad spectrum of scenarios from simple threats involving radioactive material, hacking and cyber attacks to stealing radioactive material, or even crashing a commercial airplane into an NPP.

Simple scenarios are always more likely to occur. Nuclear material for civilian use is a greater smuggling threat and even if it does pose handling difficulties, it could still be used for a crude nuclear device (Cameron, 1999). Aspiring nuclear states that face significant terrorist threats would face particular challenges in avoiding terrorist theft of fissile material in order to manufacture a dirty bomb (Miller & Sagan, 2009). When already in possession of such material, a device could be built by a small group utilising open literature and fairly elementary precautions such as a neutron counter (Cameron, 1999, p. 132).

One dimension of the hybrid threat toolbox, as identified in the Hybrid CoE and JRC report,[7] is the potential use of Chemical, Biological, Radiological and Nuclear (CBRN) agents by terrorists. The experience of the Salisbury attack by undercover Russian military intelligence operatives shows how CBRN attacks could seriously challenge national preparedness systems. Moreover, publicising the theft of CBRN agents could cause panic. The Salisbury incident and the prior Litvinenko affair in 2006 showed that materials hazardous to humans can be used for political purposes; scenarios relating to the use of nuclear materials should not be excluded. These two incidents show what can happen if CBRN material falls into the hands of terrorists.

7 *The Landscape of Hybrid Threats: A Conceptual Model* (2019) Hybrid CoE and JRC (forthcoming).

Terrorism targeting nuclear power plants poses a challenge to physical security since it goes without saying that a terrorist attack against a nuclear power plant would have grave consequences. However, the current assessments do not see it as a realistic or viable threat given that it would require a level of sophistication from terrorists that has not yet been witnessed (Ward, 2018).

The cyber domain

Today, "terrorism" and crime are often related to the cyber domain. Modern technologies have created new ways to attack and cause harm. When it comes to cyber, the application of international law to critical infrastructures in cyber events is covered by the *Tallinn Manual*, and from an international legal perspective there is no difference between cyber attacks related to nuclear facilities and those related to other critical infrastructures (Schmitt, 2017).

Nuclear facilities in general use several independent security protection systems. It should be difficult for an outsider to carry out a cyber attack that would lead to a severe situation for an NPP. The security system includes automatic shutdown in specific situations, emergency cooling and physical shields through the reactor tank, reactor housing and, as a last resort, the reactor building. Process automation and control systems manage valves and pumps, measure temperature, pressure, radiation and flow, and so on. These systems are separated from the internet and implemented through independent networks. Hence, they should not be reachable from outside of the facility. However, the Stuxnet infiltration into Iranian nuclear facilities proved otherwise.

The International Atomic Energy Agency (IAEA) has conducted a review of the Ostrovets nuclear power plant in Belarus, which is one of the power plants discussed in this study. The IAEA also refers to a Finnish nuclear power plant in the document. Their study shows that both power plants use several separate systems with different technologies to ensure safety. This means that if one safety system is affected by a cyber incident, then there should be another safety system to take over. The systems use different technologies so that two or more safety systems should not be affected by the same fault. A severe incident would only be possible if all parallel safety systems were out of order at the same time. The IT and control systems should be penetration tested with the help of independent security experts before taking the facility into production, and as a part of regular maintenance to expose design errors and known vulnerabilities.

Even though nuclear weapon programmes are not at issue here, the topic is cloaked in secrecy and one in which intelligence gathering has also played a part, while continuously evolving cyber technology provides increasingly better tools to conduct such operations. Nuclear power plant building projects have a history of intelligence operations. "During the Cold War, the United States and the Soviet Union invested heavily in intelligence activities to determine each other's nuclear strike capabilities. One avenue was recruiting technical experts and construction workers involved in nuclear infrastructure development" (Hillman, 2019). The actors may be different today, such as non-state cyber criminals or third-country industrial spies, but the threat of reconnaissance and exploitation remains the same.

If the separation of safety systems has not been implemented according to best practice, for instance if the internal control network is connected to a Wi-Fi network, to a conference room or to other facilities, then the control network could be accessed by a visitor to the plant, or from a distance, somewhere in the vicinity of the building. IBM presented an example of this during the Black Hat conference in 2006, where they outlined the penetration of a power plant through an unprotected wireless access point. This was used to gain access to the business network, and subsequently the plant's control network using an exploitation that was ten years old at that time (Kesler, 2011, p. 17).

If an external computer, USB stick or other device is connected to the internal network, then there is a risk that it could introduce malware. One example is the Slammer worm,[8] which infected computer systems at the Davis-Besse nuclear power plant in Ohio. The worm travelled from a consultant's network to the corporate network,

8 For more information on the Slammer worm, see e.g. http://cseweb.ucsd.edu/~savage/papers/IEEESP03.pdf.

then to the process control network for the plant. The traffic generated by the worm effectively clogged the corporate and control networks. For four hours and fifty minutes, plant personnel could not access the Safety Parameter Display System, which shows sensitive data about the reactor core collected from the coolant systems, temperature sensors, and radiation detectors. This did not affect analogue readouts on the equipment itself; plant technicians could still obtain reliable data from the sensors by walking over to them and reading them. (Kesler, 2011, p. 20)

It is not only the safety systems that have to be protected. In Korea in 2014, a nuclear facility was hacked resulting in the leak of personal details of 10,000 Korean Hydro and Nuclear Power workers, designs and manuals for at least two reactors, as well as electricity flow charts and estimates of radiation exposure among local residents. There was no evidence, however, that the nuclear control systems had been hacked. (McCurry, 2004) This is a good example of where the domains of information, intelligence and cyber are linked to nuclear energy.

The energy produced by an NPP cannot be transmitted without the power grids. In a hybrid threat environment, an adversary might therefore attack an NPP indirectly by influencing or attacking other parts of the electricity network. Even if the reactor part of the power production has all security measures in place, it is possible that other parts of the facility have less protection. For instance, researchers at the US Department of Energy's Idaho Laboratory ran the Aurora Generator Test with a remote high-voltage circuit breaker to physically destroy a generator by quickly opening and closing the breaker (Meserve, 2007). This shows that an uneven load on the grids could affect the power plant. Electric grids are becoming increasingly complex with the inclusion of new unstable energy sources, micropayments for energy, and so forth. This complicates the ability to obtain a full overview of the grid and to protect the control systems against both cyber and technical faults.

One of the most striking cases, the Ukrainian electricity blackout in 2015, which was the first ever known power outage caused by a cyber attack, shows that the electricity grid can be attacked by cyber means. The attack is believed to have been carried out by a persistent Russian advanced threat group called "Sandworm". The same group has been suspected of being behind attempts to hack European Union institutions, American government entities, and NATO targets, and they have recently made repeated attempts to hack European telecommunications companies, for example. "Sandworm" is known to use a distinctive hacking tool called BlackEnergy (Vijay, et al., 2017). As the case study shows, it is evident that "actors from different levels have been working on the different stages of the attack. This means that there is a possibility that this attack was done in cooperation between cybercriminals and nation-state actors – it anyway had to be done by an extremely capable and well-funded group of actors" (Vijay, et al., 2017).

Interestingly, the Ukraine case revealed a quantity of old control equipment that was not interconnected in the same way as it usually is today. This reduced the impact of the cyber attack. Today it is not uncommon for old equipment that is not made for interconnection to be connected together and even accessible through the internet to enable remote operation. Such equipment could be 20–30 years old, out of production and without available security patches. Connecting such pieces together could pose a major security risk since the old equipment was not designed with security in mind. If an attack similar to the one in Ukraine had occurred in a country with more interconnected equipment, then the blackout could have been much more severe. Also of interest is the fact that the Ukrainian nuclear facilities were not attacked at the same time but, as we saw with the power generator example, an uneven load could also affect the generators at the power station.

Information influencing activities

It is widely known that nuclear energy is a topic that divides public opinion (Rosenkranz, 2006). One of the reasons for this is that accidents related to nuclear plants and facilities usually receive a lot of attention and even more so if the reactor core has been damaged – as was the case in Chernobyl and Fukushima. The perceptions that accidents with devastating consequences such as these give rise to may well be used as a part of information influencing since energy decisions are significant and all-encompassing for a state, involving public

debates, parliamentary debates, and expert assessments of different legal and environmental issues. The media play a major role in relaying these debates and also in shaping and transmitting public opinion.

Reactions to different debates and expert assessments come from the business community, local communities and different types of interest groups. Narratives alleging paranoia and erratic behaviour are likely to be used to undermine confidence in claims made by oppositional voices. This means that the decision to build or expand an NPP is an issue that will attract a significant amount of attention from the public, the media, government entities and experts on a range of issues regarding safety, ethical, legal and environmental concerns. In this way, it can be expected that different NPP projects might be targeted not only by domestic interest groups but also by a range of activities from state and non-state actors trying to influence the decision-making processes.

Furthermore, the possibility of accidents is a significant factor in neighbourly relations. The Finnish example is a good indicator when trying to understand the effects of foreign power plants on countries nearby. Finland has long been living next door to the Russian Sosnovyi Bor power plant, and the two countries have been cooperating on the issue. Nonetheless, Finland has been concerned about the power plant's old reactors (Sipola, 2017). Sosnovyi Bor has had a similar type of reactor to the one in Chernobyl, which has naturally added an extra element to threat perceptions. The nuclear power plant is so close to the Finnish border across the Gulf of Finland that, without the opportunity for frequent visits by Finnish experts, the plant would have been seen as a major safety hazard for Finland. The Sosnovyi Bor case shows that only through transparency and openness can neighbouring countries' safety concerns be alleviated. In 2011, the Finnish Radiation and Nuclear Safety Authority conducted a study on foreign nuclear power plants, which concluded that "an accident at a foreign nuclear power plant would not endanger the Finnish water supply system. However, large areas (even thousands of square kilometres) could be contaminated to the extent that restrictions and bans would be required for food production, although it is unlikely that there would be acute health effects (radiation sickness or burns) in Finland" (STUK, 2011). The latter conclusion was dependent on weather conditions. The construction process of the NPP in Ostrovets, Belarus would benefit from similar openness and visits, as the secrecy only serves to fuel mistrust in the neighbouring area.

Media freedom is critical in ensuring that all aspects, risks and threat perceptions are taken into account. Analysing debates around critical issues and listening to different perspectives allows more knowledge to be gained, helps in distinguishing real threats from perceived ones, and allows the building of measures that mitigate the risks of potential threats.

However, the media might also be used as a space for an adversary to shape public opinion in a way that supports the interests of the adversary. An actor might want to create a positive narrative around nuclear energy and NPP construction, as Russia has been trying to do in Finland and Hungary, and as highlighted in the case studies. Such arguments are linked to green energy, the creation of jobs and promoting good social values. Rostec is also constantly building its image as a trustworthy, high-tech international partner and global leader in nuclear energy technologies. Rosatom has been very active in trying to convey a positive image of the Hanhikivi project by organising educational summer camps, flooding social media with positive viewpoints on the project, and discussing cooperation in high-level press releases. However, Finnish civil society, including local actors, the media and NGOs, has been equally active in spotting mismatches and in pinpointing the downsides of the project.

Conclusion

In the era of hybrid threats, our security environment has changed significantly compared to a decade ago. Interconnectedness and globalisation as well as new technologies have brought new methods of interfering and using influence, while traditional threats are still present and old strategies are adapted to the contemporary context. Geopolitical realities and competition among great powers and regional hegemons must be taken seriously. Energy is a potential tool for geopolitical influence. In this kind of environment, it is important

to rethink our approach to security and threats as well. Things that we do not see, hear or feel are difficult to perceive as threats. Nuclear energy is no different from oil and gas in this respect.

However, there are also specific ways in which nuclear energy can present a threat compared to oil and gas. The dual-use potential of materials required to produce nuclear power must be considered when states engage in nuclear programmes that are not wholly open, or which are even veiled in secrecy. This creates what the EU calls a CBNR-related threat, namely the possibility that nuclear material is being used in an attack against democratic states, most likely by a terrorist organisation.

In addition to providing materials for dirty bombs, there are other ways in which nuclear energy production might be used by terrorists. A nuclear power plant could be the target of a cyber attack, in which case a hostile state or non-state actor would aim to covertly disrupt or cut the energy distribution in a target country or to steal critical information. Nuclear power might also be exploited by terrorists using an NPP itself as a weapon, in the worst case by destroying it. However, it is more likely that this kind of scenario would be presented in information influencing activities with the purpose of scaring the public, rather than actually occurring.

It is also possible to attack an NPP indirectly, by causing damage to the power grids that are used to distribute energy. Such an attack would threaten the nuclear power plant by potentially damaging the generator. Moreover, it could completely cut the energy distribution. Dependency on possibly less secured energy grids is a vulnerability that ought to be considered from the nuclear energy security point of view as well.

The most prominent hybrid threat related to nuclear power is the economic leverage that is exerted through economic connections between supplier states and countries where an NPP is built. The state in which the nuclear energy is supposed to be consumed is particularly vulnerable if the whole chain of producing, refining and supplying both material and know-how is in the hands of one state or state-led company. Moreover, huge loans and long repayment periods create both economic and political ties between the states. The economic leverage could be utilised in different ways should the supplier country enter the priming phase of hybrid warfare.

The trauma of Chernobyl and the more recent accident in Fukushima were particularly instrumental in instilling tenacious threat perceptions in the public consciousness, and could duly be utilised in information influencing activities. The fear of a nuclear disaster could be exploited by competitors from other energy production fields, but also by terrorists in hybrid warfare.

Regionally, secrecy affects neighbourly relations as an NPP is both a provider of energy and a potential physical threat also outside a host state's borders. Media freedom and openness with regard to NPP construction projects and all phases of nuclear energy material production are key in mitigating threats relating to the secrecy and vulnerabilities of NPP infrastructure in particular. A good example is demonstrated by the regular visits paid by Finnish representatives to Sosnovyi Bor. Openness also affects threat perceptions as reliable information about the safety of nuclear energy is provided, thus preventing and undermining potential information influencing.

PART II:
Empirical evidence

The first section in this part of the report, written by James Henderson from Oxford Institute for Energy Studies, is dedicated to an analysis of Rosatom as an actor. Henderson concludes that Rosatom's actions seem to be in line with Russian foreign policy priorities, while commercial drivers are also part of the picture. This analysis is followed by three case studies in which Rosatom is the main player. Ostrovets power plant in Belarus has raised some concerns in neighbouring countries. The planned construction of the new Hanhikivi nuclear power plant generated much debate in Finland in 2015. While commercial aspects are central to the project, some safety concerns have been raised both in relation to the physical safety of the process as well as the long-term effects. Paks power plant in Hungary is pivotal in Hungarian energy security. The cooperation with Rosatom caused the EU to question the state aid principles. To this end, all of the case studies have similarities as well as significant differences, and all three should be viewed in relation to their own context as well as the broader European context.

Rosatom – competitive commercial actor or tool of Russian foreign policy?

The formation of Rosatom in 2007 involved the consolidation of approximately 400 individual entities across the nuclear value chain in Russia into one state-controlled body. As such, the company became a state champion alongside its hydrocarbon-focused peers Rosneft and Gazprom, conforming to the Russian industrial strategy in the Putin era of state control over key strategic industries. In addition, Rosatom also maintained the Russian state's key focus on energy exports. Oil and gas account for more than half of the country's export revenues, and the Russian economy remains heavily reliant on the global oil price as a result, but various Russian energy strategies over the past two decades have also highlighted the need to expand nuclear exports as well, in the form of both power plant construction and in the provision of fuel and disposal of waste. Rosatom has always argued that this strategy has its roots in commercial logic, being a source of international revenues and domestic GDP growth, given the wide range of industries that support the nuclear sector. However, the suspicion in many arenas has been that the high level of technological, financial and in some cases operational dependence which the use of nuclear power creates has also provided the Kremlin with a powerful foreign policy lever and a vital source of soft power. This section will discuss the various arguments surrounding this issue and will argue that a nuanced approach is required to disaggregate the various commercial and geo-political forces that are at play.

Rosatom's international activities

In the latest Energy Strategy for the Russian Federation, the export potential of Russian nuclear technology is noted and a primary objective of increasing the export of nuclear power services, as well as nuclear power plants, is set (Russian Government, 2015). In fact, this strategy had been put in place by Rosatom's leadership some time before, as in 2011 it had laid out a long-term development strategy that was largely export oriented, with specific targets for revenues from foreign operations to account for 50% of the total by 2030, and for the company to also have contracts for the construction of at least 30 nuclear units overseas (Minin & Vlcek, 2017). Emphasising its activities across the nuclear value chain, the company also wants to have a 42% share of the enrichment market and 22% of the nuclear fuel fabrication market, underlining its ambitions to become a major global player.

The company's Annual Report for 2017 suggests that it is well on the way to achieving these goals, as it claims that it already has orders for 33 power units in 12 countries around the world. In

addition, uranium products were being exported to 27 customers in 12 countries, with sales valued at US$1.7 billion, while the portfolio of nuclear fuel export orders had reached $10.8 billion for the next decade, with 2017 sales worth $1.2 billion (Rosatom, 2018). Furthermore, Rosatom has outlined its plans to develop new initiatives for its overseas markets, including expansion of its "back-end" waste processing and storage business and development of nuclear research and technology centres for scientific research. The company will also continue to offer maintenance services and employee training to those countries where the nuclear power business is a relatively new initiative.

It is interesting to note the countries where Rosatom is particularly active, as any analysis of the balance between commercial and geo-political motivations is clearly affected by the experience of each one in the nuclear sector, the current state of relations with Russia, the need for Rosatom's financial and other support, and the position of nuclear power within the country's energy system. For example, China became a customer for Russian nuclear technology in 1997, ordering two AES-91 type reactors for the Tianwan site, and since then the nuclear industry in the country has expanded dramatically. However, despite this growth, only two more Russian reactors have been ordered, essentially to expand the Tianwan site, as competition from international and Chinese domestic companies has meant that Rosatom has struggled to win new orders, despite warming relations between the two countries. China clearly does not need Russian financial support to expand its nuclear sector, removing one of Rosatom's main bargaining tools, and the country's ability to diversify its sources of energy and nuclear power supply has left Russia in a weak position. Furthermore, China has also acquired the ability to assemble fuel for Tianwan using Russian components, further reducing its security risk.

India also offers huge potential for growth in the nuclear sector, and Rosatom does have significant operations there, having built two reactors at Kudankulam which are currently in operation, with a further four plants either under construction or contracted. However, the poor performance of the first two reactors, which elicited complaints in the Indian parliament, have rather undermined Rosatom's position in the country. Nevertheless, India's close geo-political relations with Russia and the country's need for support to finance its significant growth plans in the nuclear sector may play into the company's hands in future.

Beyond these two giant markets, the rest of Rosatom's current international business is in smaller countries with varying levels of dependence on the Russian company. In Belarus, two reactors are being built at Ostrovets, funded by a $10 billion loan from Russia, and despite construction problems and start-up delays, the close relationship between the two countries leaves Rosatom in a uniquely powerful position. Another former member of the Soviet bloc, Hungary, is already a user of four VVER 440 reactors built in the 1980s, but plans to expand the site at Paks have been somewhat controversial, not least because of the EU's intervention. Again, a large loan (€10 billion) has been provided, and the newly elected government of Viktor Orbán accelerated the approval process for the new Paks-2 facility through parliament, but concerns over EU energy security, the level of interest payments and an excessive reliance on Russia as an energy partner have led to opposition protests and potential delays (Digges, 2019).

Rosatom's other current project within the EU, in Finland, has also encountered institutional barriers, not least due to an insistence on majority Finnish ownership of the project. A joint venture, Fennovoima (in which Rosatom cannot own more than 40%),[9] has been set up to own the project, but issues around licensing and other approvals have meant that construction is unlikely to start before 2020 (Aalto, et al., 2017). Another project, outside the EU, that has been delayed by partnership issues is at Akkuyu in Turkey, where Rosatom has struggled to find Turkish investors to take a 49% stake in the project. Interestingly, and to avoid further delays, Rosatom committed to a Build-Own-Operate contract (BOO) for the project, confirming its long-term commitment to the country. The first

9 66% of Fennovoima Oy is owned by Voimaosakeyhtio SF and 34% by RAOS Voima Oy (Rosatom). STUK required that at least 60% of Fennovoima's shareholders must be of EU or EFTA domicile and committed to further financing of the project.

concrete was laid in April 2018, and the first unit is expected to be operational in 2023, even though Kirill Komarov, first deputy director-general for corporate development and international business at Rosatom, has admitted that the timetable is very challenging (Tzanetakou, 2019; WNN, 2019). It remains to be seen when the NPP will actually be operational.

The first concrete has also been laid in Bangladesh at the site of the Rooppur plant, where Rosatom plans to have built two reactors by 2023/24. A US$11.8 billion loan has been provided by Russia to cover 90% of the construction cost, and interestingly India has been brought into the project via a Memorandum of Understanding on nuclear cooperation, perhaps to provide political balance for the partnership. Significant financing has also been promised for Egypt, where US$25 billion has been offered to cover 85% of the cost of four reactors at the Dabaa site. Commercial contracts were signed in 2017, with the first power expected in 2024, but it remains unclear whether construction work has actually started. Nigeria is also in the process of negotiating the purchase of four 1200MW reactors, with the full expectation that financial support would be required. An initial agreement was signed in 2017 and feasibility studies are underway, but no dates for construction or the first electricity have been announced.

Interestingly, three countries that have been in negotiation with Rosatom have now either cancelled or postponed their nuclear plans. Vietnam had announced plans for a seven-reactor site at Ninh Thuan, with Rosatom providing at least two of the reactors and Russia agreeing to lend US$7.7 billion to finance the plant. However, rising costs (a doubling of the cost of the Russian reactors to US$18 billion) and safety concerns led to the whole plan being scrapped in 2016. Jordan also announced in 2013 that it would contract Rosatom to build two AES-92 reactors under the BOO model being used in Turkey, but again issues around costs and financing caused problems, and by mid-2018 it appeared that a new plan to build small modular reactors had replaced the larger scheme. Finally, in South Africa the government announced an ambitious plan to build a total of 9600MW of new nuclear capacity by 2030, with Russian involvement seen as a major component of the plans. Indeed, it appeared that an IGA may have been signed to secure Rosatom's place in return for significant Russian financial support before this was challenged in the South African High Court and declared illegal, pushing back the plans indefinitely.

One final, but important, part of Rosatom's overseas plans involves the Bushehr site in Iran, where the company has essentially agreed to build eight new reactors in a number of stages. There has been some confusion over whether other international companies might also get involved, a situation that has been further complicated by US sanctions, while technical and financing issues have also resulted in delays. The Russian government has offered a US$3 billion soft loan, which may be allocated to Bushehr, but at present it would seem that construction work is only at a preliminary stage.

Commercial drivers and institutional constraints

This description of Rosatom's overseas activities highlights the various inter-related themes that appear to drive the company's strategy and underpin its competitive strengths, and suggests that the job of untangling commercial objectives and geo-political goals is a complex one. At its most basic, the provision of energy in any form is clearly a politically strategic priority, and therefore dependence on a third country for provision of technology, infrastructure or fuel comes with associated security concerns. In Russia's case, the example of Gazprom in Europe provides an obvious point of comparison. Indeed, it is hard to dispute that under Putin energy exports have always had a twin motivation, since the earliest energy strategy published under his presidency stated that Russia's "significant energy resources and powerful fuel-energy complex are instruments for conducting domestic and foreign policy" and that "the role of the country on global energy markets to a great degree determined its geo-political influence" (Lough, 2011).

Not surprisingly, Rosatom itself denies any link between its activities and Russia's political goals. Its leadership have often attempted to address the issue head-on, with statements such as "when Rosatom decides on a project, we are guided first of all by economic considerations. I know of no precedent for anything driving us to accept

a knowingly unprofitable project". Of course, one would expect such statements from company management, as it would be commercial suicide to admit that political influence drove any investment decisions (Minin & Vlcek, 2017). Nevertheless, the remarkable success of Rosatom over the past decade – with the company accounting for 23 of the 31 reactor orders placed between 2009 and 2018 (Thomas, 2018) – hints at the fact that some non-commercial forces may be at work, or at least comparative advantages. Indeed, it is interesting to note that so many of the company's international competitors, including Westinghouse, Areva, Toshiba, Hitachi and General Electric, have suffered significant financial losses in the sector while Rosatom has flourished (Iijama & Hotta, 2019). Its main competitors in recent tenders have been Chinese and Korean companies, and it would appear that the construction of nuclear power plants will increasingly become a game for state-supported companies. As a result, Rosatom's success is perhaps not quite so surprising.

Furthermore, there is no doubt that the company does have to abide by the rules of a competitive marketplace and is constrained by institutional regulation in the various countries and regions where it operates. National bodies govern the licensing of new plants and impose rules to control the environmental impact of any facility, and of course have the ability to negotiate on the price of electricity that is sold from the operational power station. Indeed, it is interesting to note that a number of Rosatom's potential projects in countries with good political relations with Russia (Jordan, Nigeria, South Africa) have failed due to cost and regulatory issues, while Rosatom has also demonstrated its commercial acumen in choosing where to be involved in electricity sales. It opted, for example, to participate in the Finnish electricity market, where prices are determined by market conditions, and to avoid involvement in Hungary, where low prices remain regulated by the state.

Having said this, Rosatom has a key competitive advantage as its ability to offer a service across the full value chain is unique in the industry. In one sense, of course, this increases the risk of customer dependency, but in another it enhances the company's ability to create synergy benefits and drive down overall costs. As a result, one might expect it to be able to offer more competitive construction costs, if it expects to generate further value elsewhere. Provision of fuel is one obvious area, and indeed Vlcek highlights the concerns in this area about the near monopoly which TVEL (a Rosatom subsidiary) holds over the fabrication of fuel rods for the VVER technology which the company uses in its power plants (Vlcek, 2016). Westinghouse has provided an alternative source in the past, and the European Union has provided grants to encourage alternative suppliers to develop new sources of fuel for Russian reactors, but Rosatom retains an advantage given its experience in the field and its ability to provide assurances on quality and specificity as well as cost. Moreover, it regularly closes life-long contracts for supply of fuel to Russian reactors, further consolidating its position.

One other major advantage, which is prevalent in many of the examples noted above, is the ability of Rosatom to provide financial support (via the Russian state) to countries considering the purchase of a Russian-made reactor. Indeed, the ability to offer large loans also has a commercial benefit, as the interest rates charged can generate significant profits. For example, the US$11.4 billion loan to Bangladesh is set to generate US$8 billion in interest payments, while the US$25 billion loan to Egypt could ultimately lead to the country paying over US$70 billion to Russia over the 35-year term (Digges, 2019). Despite these apparently exorbitant terms, however, many countries rely on the ability of companies to provide financial support from their host governments in order to be able to fund the high up-front costs of nuclear power stations, and the Russian government seems keen to help. While politics may well play a role, there are also good domestic reasons for providing loans, which in Russia's case often come from the National Wealth Fund that is meant to be invested for domestic pension provision. This can be justified by the fact that the nuclear sector generates significant economic wealth in the form of GDP growth, employment opportunities and the basis for corporate expansion in multiple supporting industries. In addition, it also provides Russia with a clear global technological strength and prestige at a time when sanctions are limiting opportunities for development in other energy sectors.

Links to geo-politics and soft power

However, while it is certainly possible to explain Rosatom's activities in commercial and competitive terms, it would be naïve to suggest that there is no element of politics involved. Nuclear as part of the Russian strategic energy sector also has political priorities. As one of only seven strategic "state corporations" the President of Russia appoints the company's Director General and members of the Supervisory Board while the government approves the company's long-term strategy, and therefore company management is clearly motivated to keep its political masters happy. Furthermore, the list of countries where Rosatom is active includes many important strategic partners of Russia: China, where energy exports are becoming a key foundation for political relations; India, with a long history of friendship with Russia; Turkey, where relations have sometimes been better and sometimes not so good, but where energy provision and transit services to Europe create the potential for a solid long-term partnership; and Iran, where long-term friendship and anti-US sentiment are underpinned by energy diplomacy. The provision of a mixture of finance, technology, and energy supply to all of these countries, and others described in section one, offers the chance for a long-term strategic relationship that can be further enhanced by the contractual nature of Rosatom's business. The use of BOO contracts, for example, implies a business partnership lasting the multi-decade life of the nuclear plant that has been constructed.

This does not mean that all of these countries are beholden to Russia, of course. Some, like China and India, have multiple energy options and their economic strength and growth potential make them attractive to multiple energy suppliers. However, other economically weaker countries (perhaps Egypt and Bangladesh as examples) may be more susceptible to the lures of a Russian commercial offering that comes with political strings attached. As noted above, however, commercial reality must still be respected, given the examples of countries that have ultimately scrapped their nuclear plans due to cost or pricing issues.

Nevertheless, it is interesting to note that Russian political leaders do like to use Russia's expertise in the nuclear power sector as a gambit in political discussions with potential partners. In December 2018, for example, President Putin discussed the construction of nuclear reactors in Argentina using Russian technology with President Macri as he sought to develop relations with a key South American ally (WNN, 2018). Meanwhile, Energy Minister Novak has announced that Rosatom will apply for a tender to build a nuclear power plant in Saudi Arabia (De Clercq, 2017), which is becoming a key Middle Eastern partner for Russia with developing energy ties in the oil and gas sectors via alignment on OPEC production deals and potential investment in Russian LNG schemes. Finally, Prime Minister Medvedev has announced Russia's willingness to take part in a tender for the Belene NPP in Bulgaria (Soldatkin & Nikolskaya, 2019) at a time when negotiations on key gas pipeline infrastructure are also at a crucial stage, and Russia has also signed an agreement on the peaceful use of nuclear technology with Serbia during a visit by President Putin to the country, while Rosatom has announced the construction of a centre for nuclear science in the country (WNN, 2019). Serbia could also become a key transit route for Russian gas to Europe once the new Turkish Stream pipeline opens in 2019/2020. While it is of course possible that all of these activities are independent of broader political goals, the coincidence of nuclear power discussions with key current and future allies is hard to ignore.

Conclusion

Rosatom has arguably been the most successful exporter of nuclear power technology in the world over the past decade, as many of its competitors have fallen by the wayside. Its success has undoubtedly been due in part to its unique offering across the nuclear value chain and its ability to provide competitive costs (albeit sometimes still not low enough), and it also seems undeniable that commercial logic and compliance with national and regional legislation and regulation do facilitate and constrain the company's activities.

However, it is also clear that Rosatom's activities, and the support that it receives from the Russian state, also have a political motivation. Domestically, the industry provides a source of economic growth and employment, while overseas it can enhance Russia's prestige as a technically sophisticated industrial power. In addition, however, the

coincidence of Rosatom's business with key current and future allies of Russia, and the obvious strategic nature of any long-term nuclear deal, confirm the political undertones of much of the company's activity. Commercial reality can provide a check, and in a number of instances has already done so, but the reality that China is slowly becoming Russia's competitor in the nuclear sector underlines the fact that geo-political drivers are clearly a vital element in determining success in the sector.

Ostrovets nuclear power plant – case study

Nuclear energy trade is not as politicised an issue in Belarus as oil or gas trade with Russia. The oil sector constitutes a large share of the bilateral trade and is a direct way for Belarus to receive foreign currency and revenues. Russia exports cheap crude oil to Belarus, where two companies, the 100% state-owned "Naftan" and "Mozyr Oil Refinery" (42.581% owned by the Russian Gas Company "Slavneft"), are the main players. The crude is refined and further exported to countries such as the Netherlands, Ukraine, and Latvia (Uniter, 2012). As Margarete Balmaceda has shown, the Belarus government has prioritised the modernisation of its oil refineries to increase production of oil products and gasoline that comply with EU standards (Balmaceda, 2014). However, due to reforms in the Russian crude oil taxation system that will include raising the mineral extraction tax, Belarus is facing an overall loss (including multiplying effects) that could exceed $1 billion a year (Preiherman, 2018). This translates into a large economic leverage for Russia. Gas has been even more important when it comes to Russia-Belarus relations since Belarusian heating and electricity production is 90 per cent dependent on Russian gas.

In its current energy strategy, Belarus is set to diversify its energy portfolio away from the current heavy reliance on Russian gas. In addition to nuclear capacity, the strategy includes the construction of a coal-fired plant, hydropower stations and wind projects (WNA, 2019). Even if all fuels – oil, gas and fuel rods for NPP – still originate from Russia, nuclear energy could be considered more stable, and less exposed to sudden regulatory changes and market fluctuations.

The controversy of the location

The interest in increasing the role of nuclear energy in the Belarusian energy mix has existed for a long time. In the early 2010s, the building of Ostrovets nuclear power plant (NPP) was announced, and was seen as the bright hope of the Belarusian energy sector (Smok, 2016). Out of the initial 74 locations identified in the early 1980s, in December 2008, Ostrovets, around 20 kilometres from the Lithuanian border and 40 km from its capital Vilnius, was selected by Belarus as the most suitable site for the NPP (IAEA, 2017). The decision to locate it so close to an international border and to the capital was not well received by neighbouring Lithuania. Furthermore, there were also some question marks over how well the building project itself had followed international regulations. The IAEA visited the site as late as 2017, when 70 per cent of the project was complete (Morgan, 2017). Another noteworthy aspect is that the building project also included a 300-man-strong military presence to guard the site. These soldiers had been trained in St. Petersburg by the Russian national guard (Česnakas & Juozaitis, 2017). In addition, an anti-aircraft missile regiment was stationed near the site with a TOR-M2 anti-air defence system, and new radiolocation military and mobile radars (Ioffe, 2018), duly increasing the military presence close to the border between Lithuania and Belarus. As the Zurich Centre of Security study report notes: "these steps can be interpreted as attempts to protect Ostrovets NPP from terror attacks, but they also strengthen Russian anti-access/area denial (A2/AD) capabilities in the BSR and create additional issues for airplane traffic. Many flight routes to and from Vilnius International Airport cross the NPP area, and the close proximity of Vilnius airport to the Belarusian border and the NPP increases the chance of incidents" (Česnakas & Juozaitis, 2017). None of the pieces in the puzzle pose a direct threat, but the potential is there and together they start to form a picture that lends support to Lithuanian concerns.

As early as 2011, Lithuania raised concerns over security and safety issues relating to the Ostrovets NPP. This is very much in line with the way in which NPPs close to national borders are also a matter for their neighbours, not only for the country that is building the plant. The statements from the Belarus

side also indicate that they are aware of this factor as Vladimir Makei, Belarus's foreign minister, has said that Belarus will co-operate with the EU and be transparent about the Ostrovets plant (Peel, 2017).

Yet despite the Belarusian statements, security concerns continue. In April 2017, Lithuania adopted a law forbidding any electricity generated in the unsafe Ostrovets NPP access to the Lithuanian market. Lithuania also denies Belarus access to its electricity grids for electricity exports to other European states (Lithuanian MFA, 2018). Soon after, Lithuania passed a law that recognised the Ostrovets NPP under construction as unsafe and as posing a threat to the national security of the country, its environment and public health (Lietuvos Republikos Seimas, 2017).

In February 2019, the United Nations Economic and Social Council adopted a decision on the Convention on Environmental Impact Assessment (also known as the Espoo Convention), where it states that Belarus had failed to provide the Committee with all necessary information regarding justification for the selection of the Ostrovets site over the alternative sites (UNECE, 2019). This had already been requested by Lithuania in the decisions made by the Espoo Convention in 2014 (UNECE, 2014).

Other issues related to Ostrovets

Location was not the only problem related to the Ostrovets NPP. Non-compliance was noted several times by the Meeting of Parties to the UNECE *Convention on access to information, public participation in decision making* (Aarhus Convention). The most recent decision on Belarusian non-compliance is from 2017 (UNECE, 2018).

The EU peer review report on the Belarusian 'stress tests' (July 2018) revealed that a comprehensive seismic assessment of the site had not been performed prior to the preparation of the NPP design, although Belarus had committed to this in 2011 (ENSREG, 2018). The seismic assessment is crucial in order to determine appropriate NPP design criteria. Other serious identified deficiencies in the NPP design related to possible loss of safety functions, and shortcomings in severe accident management (ENSREG, 2018).

The IAEA Integrated Nuclear Infrastructure Review (INIR) of 2012 recorded Belarus's intentions to ratify the Amendment to the Convention on the Physical Protection of Nuclear Material, but this has not been done as yet. In 2016, the IAEA Integrated Regulatory Review Service (IRRS) noted particular gaps in Belarus's nuclear safety and oversight framework. In 2018, the IAEA Emergency Preparedness Review Service (EPREV) observed that regulations in Belarus do not reflect the most recent updates in the IAEA safety standards.

Construction of the NPP in Belarus has been dogged by recurrent incidents. The most serious occurred in 2016 when a reactor vessel was damaged and subsequently replaced after international pressure (WNN, 2016; Wesolowsky, 2016). Considering that Belarus is a country with an authoritarian state system and a culture of repression and discrediting unwanted criticism, there is a credible risk that in the event of an accident, Belarus might try to 'save face' rather than announce the incident and implement early civilian contingency and crisis management measures. This is amplified by the fact that Belarus aims to be recognised regionally as a reliable, technologically advanced country.

Matters are not made any easier due to the fact that there is no long-term data on the safe functioning of the current NPP design used in Ostrovets (ENSREG, 2017). The two reactors in Belarus are AES-2006 units using V-491 reactors, the latest designs in the line of VVER plants. The only operating unit with the same design is in Novovoronezh Nuclear Power Plant II in Russia, where the reactor has been in commercial operation since 2017. The same design is either under construction or proposed for sites in Sosnovyi Bor in Russia, Temelin 3–4 in the Czech Republic, and Hanhikivi 1 in Finland. An obvious security concern relates to the operating of new third-generation nuclear reactors in a country that has no prior history of adequate security and accountability measures in supervising the operation of nuclear plants.

Russian or Belarusian project?

As part of the Union State, Russia enjoys a privileged position in Belarusian foreign policy decisions and economic dealings. The Ostovets NPP is thus a Belarusian energy project that is indisputably intertwined with Russian state authorities and operators. Various Russian state-owned

companies are responsible for the financing, construction, training (BelTA, 2019), and fuel supply of the project throughout the life-cycle of the plant.

The customer and operating organisation of the plant is Republican Unitary Enterprise "Belarusian Nuclear Power Plant" (RUEBNPP) and the main functions of this enterprise are to "ensure the construction and commissioning of the nuclear power plant, its safe operation, uninterrupted output of electric power, other activities aimed at fulfilling the reported indicators, and making a profit" (IAEA, 2017). The Russian State Atomic Energy Corporation "Rosatom" is defined as the strategic partner in the NPP construction. The general design and development of the project, and key technology elements are all provided by Russian enterprises. The investment mechanism in place is government-to-government financing in the form of an intergovernmental loan and delivered on a turnkey basis.

In Belarus, the intergovernmental model means that Russian state-owned Vnesheconombank (VEB) and Belarusian commercial bank Belvnesheconombank (BelVEB) signed an agreement to implement the Russian export credit facility. Russia would finance 90% of the contract between Atomstroyexport and RUEBNPP – up to $10 billion. The payback period for the loan was settled at 25 years (WNA, 2019). The worrying development of economic leverage has been addressed. A 2017 report by the World Bank states that the Ostrovets NPP will improve the energy security of Belarus by diversifying its sources, but that "there is still uncertainty regarding use of the power from the new Belarusian nuclear power plant, the cost structure of electricity, and the mode of debt repayment" (World Bank, 2018). An IMF report, on the other hand, raises concerns about the impact of Russia's new energy taxation system or "tax manoeuvre". The report states that in the absence of full compensation for the losses of this policy to Belarus by Russia, the new taxation would have a considerably negative impact on the overall growth of the Belarusian economy (IMF, 2019). The latter statement also gives a reason to suspect that Russia's tax manoeuvres pushed Belarus to accept the project in order to diversify its sources of energy. However, considering the financing of the NPP, diversifying energy sources is not equivalent to diversifying away from dependence on Russia. This is a good example of how economic leverage can be built.

Since nuclear energy and politics are inseparable, relying on one state actor for the entire contracting, supplying and financing process can subject the customer to unnecessary political leverage exerted by the provider as already mentioned in part one. In the case of Ostrovets, there is a risk of Russia using the 25-year loan for political coercion. The means of doing this may include raising the interest rate, renegotiating worse loan conditions, discrediting the creditworthiness of Belarus, or raising concerns over the commitment of Belarus to assuring the safety of the NPP.

There has been some speculation that one objective of an adversary might involve using political coercion to harm the synchronisation process of the Baltic states with Central Europe. Russia might be tempted, should the political winds turn that way, to use the NPP as an energy weapon to coax the Baltic states into continuing market flows of electricity from Russia and Belarus during and after their electricity network synchronisation process with the Central European network. Russia could also cut the Baltic states off from the network before they are ready for it. The successful Kaliningrad isolation test proved that Russia has sufficient reserve power capacities in the enclave for independent operation (ERR, 2019). This raises the potential threat aspect of the Ostrovets NPP project for the Baltic states.

Other means of economic leverage related to hybrid influencing could include maintaining regulatory changes in the operating environment for Lithuanian investors in Belarus, making a decision to reduce the trade flows of goods through the Klaipeda port, or pitting the Baltic states against each other in a bidding contest for port use, thereby damaging their mutual relationship. Moreover, it would provide an opportunity to utilise hostile narratives, for example to accuse the Baltic states of unfair trade policies, and accuse the EU of pushing Belarus towards Russia.

Conclusion

Seeking to diversify its energy mix, Belarus has chosen to build the Ostrovets power plant. Given the alternatives for Belarus relating to

construction of the power plant, Russia and Rosatom are the obvious partners. The project is a turnkey project, which is Rosatom's usual package deal. However, as stated earlier, turnkey projects carry risks. Ostrovets is in Belarus and hence the project is not bound by EU regulations. What this would mean in terms of hybrid threats is that priming phase activity would manage to create strong leverage, which could be exerted if needed.

The threat perception related to the Ostrovets NPP derives from processes that are not wholly transparent, and questions concerning international safety standards. Historical memory and knowledge of Soviet power plants, authoritarian traditions and unclear motives for choosing the site so close to the border with Lithuania and the EU are issues that might enable the use of hybrid threat tools.

Even without non-compliance and secrecy, the construction of an NPP attracts and motivates many stakeholders to participate in public debates. Hence, as explained in the chapter on information influencing activities, there is fertile ground for hostile narratives. Information influencing activities could benefit from these controversies and secrecy. Moreover, new technologies, especially cyber, create dependencies and channels that can be used for intelligence operations and, in the worst case, for disruptions and interference in energy grids.

The diversification of the energy mix by building the NPP will not decrease Belarus's dependency on Russia, as it is the main financer of the project. On the contrary, the NPP gives Russia even greater leverage over Belarus. In a conflict situation, Belarus could be used as a Russian proxy actor. In a hybrid threat scenario, the strategic goal of the hostile actor is blurred. Real targets would be disguised: priming would take place in one country and the destabilisation phase would be executed in a completely different country.

Observations about the Ostrovets case study

- **As in the Finnish case relating to Sosnovyi Bor, transparency and openness are essential for alleviating security concerns. Increased international awareness and surveillance by actors such as the IAEA, and continued site visits by NATO nation representatives are also essential. Efforts should duly be made to increase the openness and collaboration between Belarus and neighbouring countries, the EU and NATO.**
- **Desynchronisation from BRELL would allow the Baltic states to synchronise with a bigger, more stable, and ideologically and politically more fitting network, which would mitigate the risks deriving from dependency on a Russian-controlled NPP and grid balancing service.**
- **The military presence in the region under the pretext of the Ostrovets NPP poses a potential threat. Lithuania has become more vulnerable as a result. This aspect should be considered in defence planning both in Lithuania and within NATO.**
- **When observed through the hybrid threat lens, the Ostrovets case study provides grounds for considering how action in one place/country can affect and weaken a completely different country. More research should therefore be conducted on and attention paid to this aspect.**

Hanhikivi nuclear power plant – case study

Nuclear energy is one of the main factors in Finland's achievement of greater energy self-sufficiency – a cornerstone of the country's energy security policy. In this respect, upon its completion, Hanhikivi 1 will make a major contribution to the electricity market.

Nuclear energy currently represents 33% of Finland's total energy generation. There are currently four NPPs in operation, two of which (Loviisa 1 and 2) will cease to operate in 2027 and 2030 respectively. Olkiluoto 3 and Hanhikivi 1 are needed to replace the NPPs with expiring licences. Based on the assumption that the two new NPPs will be operational, the Finnish government's commitment to renewable energy, and taking into consideration the EU's policy on renewable energy, the TEM report predicts that Finland's self-sufficiency will increase from 55% in 2018 to 70% by the end of 2030 (TEM, 2018).

Hanhikivi NPP

In 2007, Fennovoima was founded as a joint venture by four companies – Outokumpu, Boliden,

Rauman Energia, and Katternö – for the purpose of building a new NPP. A joint nuclear power plant was seen as an improvement to Finland's energy self-sufficiency. On completion, the plant is set to produce 10% of Finland's electricity. The German energy company E.ON (with 34% of shares) was chosen as the main partner for supplying the technology for the project (Fennovoima, 2018).

Fennovoima submitted its application for a Decision-in-Principle to the government for permission to construct the NPP in January 2009. This was granted in May the following year, and parliament approved the decision in July. The government approved Pyhäjoki as the construction site for the new NPP in October 2011, after declining the other two alternatives, Loviisa and Simo (WNA, 2019). The approved application, which was favourably assessed by both STUK and TEM, proposed two potential suppliers: Toshiba and Areva, an NPP constructor owned by the French government and involved in the construction of another NPP in Finland (Olkiluoto in Eurajoki).

Fennovoima received tenders from Areva and Toshiba in 2012. In October, E.ON, the technology provider and one of the main financers, decided to withdraw from the project. Several Finnish partners withdrew as well. One of the main reasons for this was the Fukushima nuclear disaster in March 2011 (Fennovoima, 2018; Ожаровский, 2016), which changed public opinion about nuclear power, and duly influenced the decisions of companies in the field as well. There were also some concerns about profitability. The Finnish media speculated extensively that the Hanhikivi project would collapse due to a lack of funding, technological know-how, and poor planning.

Change of ownership and NPP design

In 2013, Rosatom was invited to submit its tender in addition to Toshiba and Areva. In December, Fennovoima and Rosatom's subsidiary signed a co-operation agreement on the NPP. The new deal involved a new set of conditions: the NPP project would have a reactor delivered by the Rosatom group (VVER-1200), which would run on Russian fuel. The NPP contract entails buying uranium from Russia for ten years to operate the plant after its completion. In 2014, Fennovoima transferred 34% of its shares to RAOS Voima Oy, Rosatom's Finnish subsidiary. The remaining 66% of shares were left to Voimaosakeyhtiö SF, a consortium of Finnish companies (incl. Fortum, Outokumpu and SRV). The idea was that the two partners would fund the project (Fennovoima, 2018; Ожаровский, 2016). The new main contractor was set to be the Russian Titan-2, which is also responsible for building an NPP with similar technology in Sosnovyi Bor (Песчинский, 2017).

As the nuclear power plant type had changed, the environmental impact and security assessments had to be re-evaluated by STUK and TEM. In 2015, Fennovoima submitted the construction licence application, which requires a positive safety assessment from STUK. From 2015 until now, STUK has continuously asked Fennovoima for additional materials on the design of the NPP, its organisation, and for management to prove its adherence to Finnish safety requirements. As STUK has not been satisfied with the materials provided by Fennovoima, the matter has been the subject of an ongoing debate, and the process has stalled as a result.

In February 2019, the NPP project was estimated to be eight years behind schedule. When the project was initiated, the NPP was expected to become operational in 2020. However, after multiple delays in procedures, the plant is now estimated to start functioning in 2028 (Hukkanen, 2019), which may still be subject to change.
Fennovoima has been unable to provide STUK with adequate documentation on nuclear safety, and Rosatom has been unable to adapt its security practices for Finnish purposes, according to national broadcaster YLE. Work on the power plant cannot proceed before STUK receives sufficient data about the construction process and its operation (Hukkanen, 2019).

According to the contract, Rosatom will deliver the NPP and Fennovoima will subsequently be responsible for operating it, making Hanhikivi NPP a turnkey project. Fennovoima's CEO, Toni Hemminki, is of the opinion that Rosatom is responsible for providing the necessary planning documents. One of Fennovoima's experts on nuclear energy sees that the whole issue is related to the transformation of the nuclear energy sector in general, with procedures becoming more stringent than before. Greater attention is being paid to scrutinising the

project plans, design and rationale, as well as the people involved (Hukkanen, 2019). STUK's Deputy CEO, Tapani Virolainen, has commented that one of the explanations for not receiving the documents on time is the difference in working cultures between Finland and Russia. Both he and Hemminki recognise that in Russia, documentation appears after the work has been carried out, whereas in Finland the documentation needs to be in place before the project can go ahead (Vuorikoski, 2019). STUK is still concerned about the fulfilment of safety requirements, stating that the Hanhikivi NPP does not fulfil Finnish stipulations in this respect, and has failed to deliver the necessary documents. According to a quarterly safety review published by the agency in October 2018, the "safety culture" of Fennovoima has not improved and the situation is worrisome. STUK has asked Fennovoima to perform further audits as a consequence (YLE, 2018).

Political pressure and debate on ownership

With the acquisition of 34% of Fennovoima's shares by Rosatom, the company was ready to finance the Hanhikivi project to the tune of 5 billion euros – the total cost of the project being 7 billion euros. 2.4 billion of this would come from the National Wealth Fund of the Russian Federation (NWF). The NWF is "dedicated to supporting the pension system" to guarantee its long-term functioning and its "primary assignments are to co-finance voluntary pension savings of Russian citizens and to balance the budget of the Pension Fund of the Russian Federation" (Ministry of Finance of t he Russian Federation, 2019).

With the application pending, Fennovoima has gone ahead with the construction despite the fact that an instrumental part of the equation (ownership and technology) has changed. In 2015, the Finnish government made it clear that it requires at least 60% domestic ownership (which was later specified to mean EU or EEA states). This prompted discussion and political debate in the media and within government as there was uncertainty related to whether the 60% bar could be achieved or not after the withdrawal of E.ON. Voimaosakeyhtiö SF has been reassuring the Finnish public that the political will and resources exist to achieve 66% European ownership (Tikkala, 2015). NGOs that oppose the project, such as Greenpeace, have argued to the contrary. Greenpeace has emphasised that one more partner would jeopardise the whole venture. The organisation also encouraged local representatives to initiate withdrawals, so that the share of Finnish ownership would fall short of 60% and the project would be cancelled (Tiainen, 2017).

In the midst of the ownership debate, there was a peculiar incident involving an enterprise purporting to be a Croatian energy company, Migrit Solarna Energija, which appeared "out of thin air" to provide a "European" investment of 159 million euros for the project. However, the case was quickly picked up by Finnish and even international media, which identified the company as a Russian strawman with owners linked to the Russian banking sector. After requesting an assessment of the company, TEM denied its eligibility as a "domestic owner" (Ercanbrack & Burmistrova, 2015). In this instance, the role of investigative journalism was key in bringing the matter to general attention.

In 2015, the Russian newspaper *Kommersant* published an online article stating that Rosatom had found a European partner that could invest in Fennovoima in order to fulfil the government requirement of 60% domestic (EU/EEA) ownership. According to *Kommersant*, a similar method was also used in the case of the Bulgarian NPP in Belene, where Fortum and Altran Technologies were invited to participate. The article further acknowledged that the fact that Migrit Solarna had Russian owners and did not possess any technological know-how might be a deal breaker, referencing Finnish Greenpeace Director Sanni Harkki. The article also stated that Rosatom had hoped that Fortum would purchase a stake of up to 15% in the Hanhikivi project, which did not materialise due to the failed negotiations between Gazprom and Fortum over TGC-1,[10] and which was set as a condition for Fortum's purchase of the Hanhikivi shares. Further, the article stated that time was running out for the fulfilment of the ownership requirement – indicating that something needed to be done in

10 TGC-1 is a regional producer of electricity and heat in Russia with 51.79% of shares held by Gazprom and 29.45% by Fortum.

order to ensure the actualisation of the NPP project (Kommersant, 2015). In light of this, it would appear that Rosatom and thus the Russian government were openly looking for partners that could invest in the project, duly supporting the argument that the implementation of the Hanhikivi project is in the interests of the Russian state.

Journalist Lauri Nurmi has analysed the debate relating to political pressure and the Hanhikivi project in his book about Finnish President Sauli Niinistö. He argues that Fortum was pressured into acquiring shares in the project to ensure the 60% domestic ownership threshold. Fortum finally acquired 6.6% ownership shares of Fennovoima in August 2015 despite the fact that Fortum had no such plans initially and the negotiations with Gazprom over TGC-1 had failed. In a statement explaining the purchase, it was stated that the NPP project was important for Finnish society (Nurmi, 2018). To confirm how the Russian state was following the process, President Putin took up the matter in December 2015 at his annual press conference, saying that Fortum had resisted any sabotage attempt and shown readiness to work with Rosatom and assume the risks (Martikainen & Vihma, 2016, p. 7).

Nurmi assessed Fortum's acquisition of shares as a conciliatory step to ensure good bilateral ties, and as one that was taken by Fortum under pressure from the Russian and Finnish governments (Nurmi, 2018). This is an indication that business deals can escalate into state-level disputes with potential threat elements, and that energy policy can be linked to political issues in other domains. Evidence of this can also be seen in the Finnish Security Intelligence Service's (SUPO) annual report published in April 2016, which stated that foreign states had tried to influence Finland's energy politics in 2015, but which refrained from specifying which foreign actor was in question and which decisions were the target of influence attempts (Palomaa, 2016). Furthermore, as senior associate fellow at the Royal United Services Institute Mark Galeotti has warned, Hanhikivi could be used for covert operations and as a base for intelligence personnel (Ilta-Sanomat, 2019). This bears similarities to the Ostrovets case study and also shows how strategic business deals and sectors have a strong and even a hard security dimension. In other words, security should not be separated from the economic domain.

The nuclear project has also attracted attention from radical movements. "Stop Fennovoima!" is what appears to be a radical activist group protesting against the project. The group is sponsored by an international network of somewhat radical, anti-fascist "environmental" organisations that have engaged in hooliganism against mines and nuclear power plants. The "Stop Fennovoima!" group has also organised camps and protests in Pyhäjoki against the NPP through its website. In addition to its international support, the group also seems to have direct connections to Russia. For instance, Russians have been involved in the camp activities, and the website has posted statements by Russian environmentalists against nuclear energy.[11] There have also been other cases where radical groups have been "allowed" by Russian authorities despite having a somewhat "anti-Russian" narrative. If this was the case for this group, it could be a part of Russia's priming activities in a strategy designed to create or strengthen dividing lines inside the target state society. However, ascertaining whether or not the Russian authorities are aware of this particular group and its activities calls for further research.

Fennovoima and Rosatom, for their part, have naturally engaged in activities to enhance their public image by issuing positive statements about the project and organising activities for local communities to familiarise themselves with the undertaking.

This analysis shows that the NPP debate has caused controversy within Finnish business as well as within the government. Likewise, it is clear that in this case politics and business have become intertwined. It is also worth bearing in mind that it is very difficult to keep state-level politics out of energy-sector business, since some level of government involvement is often needed (with regard to permits, for instance). The picture becomes even more complicated if an outside actor has a clear strategic state interest in the activities.

11 See https://stopfennovoima.com/fi/.

Conclusion

When the issues relating to the Hanhikivi power plant building process are summed up, the list of ways in which the plant could be used as a tool by an outside actor is a lengthy one. The Hanhikivi case quite clearly demonstrates how unprecedented events can turn the project design into something quite different from what was originally intended. When the project design changes, new security and safety concerns enter the picture. There are elements attached to the Hanhikivi project that are naturally a cause for concern, specifically from the hybrid threat point of view and when considering priming activity. There are also controversial issues relating to how the project partners came about, and even some speculation that the Finnish government was put under pressure. If one wants to speculate even further, a potential attempt to destabilise the EU's unity can also be detected. There is no direct evidence of this, although an abundance of research and analysis has been conducted on Russian energy policy and its aims towards the EU. Martikainen and Vihma, for example, point out that "Dividing the EU with energy is useful for Russia, as it portrays the EU as weak and disunited, one of Putin's long-time catchphrases. It underscores Russia's economic muscle and shows that Russia still has friends in Europe, even after the Ukraine conflict and heightened tensions. In addition, splitting the EU ranks enables Russia to negotiate on a bilateral basis and thus assume flexible rules and energy contracts that favour the supplier" (Martikainen & Vihma, 2016, p. 4).

This type of pressure or wedging attempts of this sort would be seen as a destabilisation attempt in the hybrid threat landscape, since we are talking about an influence operation targeted at the internal affairs of a country or an alliance. The Hanhikivi case also begs the question of whether there was a destabilisation attempt in the form of trying to change the business culture and challenge the rule of law. To this end, nuclear energy is clearly a topic that creates dividing lines in democratic societies – divisions that can ostensibly be exploited by an outside actor even after the project is completed.

Observations about the Hanhikivi case study

- **Security challenges arise when a project partner originates from a different rule of law culture. This is a factor that should be highlighted more effectively in public-private cooperation.**
- **When a project has national strategic importance for Russia, state involvement can be expected. The objective can be two-pronged in this respect: influence the state in question and challenge the EU's or NATO's unity.**
- **Economic and security factors should not be separated, especially when the project in question involves an authoritarian state that has strategic interests in one's country and region.**
- **From the point of view of hybrid threats, even one business deal can have a strong impact on future leverage, with implications beyond the local level. Hanhikivi is a good example of how a local-level project can escalate to the state level and beyond, if hybrid activity is involved. Local-level authorities should be made aware of this eventuality.**

Paks nuclear power plant – case study

The Paks Nuclear Power Plant Company was founded on 1 January 1976, duly introducing nuclear energy into Hungary's energy mix. It was later transformed into MVM[12] (Shentov, 2018) Paks NPP Ltd, which manages the four existing reactors. The first unit became operational on 28 December 1982 and the fourth on 16 August 1987. A service life extension programme was conducted and the existing units have obtained extension licences: unit 1 will be in operation until 2032, unit 2 until 2034, unit 3 until 2036, and unit 4 until 2037 (WNA, 2019). The site was selected with an option to increase total capacity to 6000 MW, so the first ideas concerning the building of additional units were discussed in parallel with the construction (MVM, 2019).

In the aftermath of Chernobyl, and at a time when the Soviet bloc was collapsing in 1988, plans

12 State-owned MVM (Hungarian Electricity Works) is the dominant player in the Hungarian energy market in both the electricity and gas sectors, including a major long-term supply contract with Gazprom.

for further extension were put on hold. There was an attempt to prepare a tender in 1997 but MVM rejected the proposed extension due to its non-compliance with the government policy at that time (WNA, 2019). However, the idea for further extension was never completely discarded. In 2008, the Hungarian parliament adopted an energy policy strategy, following the international trend and recognition of the need for emission-free energy. In the framework of this document, it was decided that preparations would get underway for a decision by parliament regarding the construction of new nuclear capacities (Katona, 2009). The decision was adopted with an overwhelming majority in March 2009 (ibid.), one year before the current Hungarian prime minister, Viktor Orbán, a supporter of closer ties with Russia and a critic of the EU, assumed office. The nuclear energy policy is clearly a continuation of the overall policy of the government.

Russia's involvement in Hungary's nuclear energy sector is also linked to the cooperation in the overall energy sector between Russia and Hungary. The affordability of gas and electricity became an issue in Hungary in the aftermath of the 2009 gas crisis, and energy prices have been rising ever since. The Fidesz government introduced a moratorium on gas and electricity prices after winning the election in 2010, and a policy to further decrease consumer prices continued throughout 2013. These policies helped to maintain the popularity of the party and Prime Minister Orbán in the 2014 elections. Yet such policies would have been financially unsustainable without Gazprom's concessions. Between October 2013 and March 2014, at the same time as the Paks extension agreement, Gazprom made the necessary concessions vis-à-vis its export prices (Shentov, 2018, p. 144), which breathed new life into the continuation of the popular Fidesz price policies. Both the gas concessions and the Paks agreement were timed to coincide with the elections and gave the ruling party a "boost" to maintain its popularity (Deak & Amon, 2015, pp. 87, 89-90). Such financial incentives on Russia's behalf are embedded into Russia's energy policy in Hungary, and can be seen as Russia's way of building economic leverage, and as a tool through which exchanging political favours may be forced.

The agreement between the Hungarian and Russian governments for the extension of the Paks NPP was signed in January 2014. The extension will add two 1200MW reactors to the existing four. All six would be of Russian origin – constructed by a company that is part of the Rosatom group or its Soviet predecessor. The new reactors should be handed over from the constructor to the operator after the completion of all necessary testing and licensing, under a turnkey contract. Initially, the completion and commercial operation of the new reactors was foreseen to be by 2025 and 2026. Despite the initial optimism, experts involved in the project have leaked indications that the Paks NPP will not be operational until 2032, instead of the 2026 deadline planned at the start of the project (IntelliNews, 2018). If this deadline is met, a smooth transition of generation would still be possible, but further delays may cause a deficit in the Hungarian electricity market that would most likely result in electricity imports.

Negotiations

Originally, negotiations were conducted for financing and construction with three competing bidders – Areva (France), Westinghouse (USA/JPN) and Rosatom. Hungary offered to pay €2 billion out of a total sum of €10 billion. The scales were tipped by the Russian side offering to cover all of the expenses with a loan, so the share of Russian capital in the project is 100% (Aalto, et al., 2017, p. 402) on rather generous terms. Hungary will begin repayments on the loan only once the new reactors are up and running in 2026, and will repay the loan over 21 years (Than, 2015). Until 2026, the interest rate will be just under 4 per cent, rising to 4.5 per cent afterwards and 4.8 to 4.95 per cent in the final 14 years (Than, 2015). By way of comparison, the annual interest rate of the Ostrovets loan is 9.5 per cent (Morgan, 2017).

A Rosatom subsidiary originally concluded a 20-year exclusive nuclear fuel supply agreement. This was cut to 10 years after the Euratom Supply Agency and the European Commission intervened to ensure compliance with existing rules and competition among fuel suppliers (Aalto, et al., 2017, p. 402). This was an administrative exercise and did not delay the project to any significant extent (Ostrowski & Butler, 2018).

After signing the intergovernmental agreement, the negotiation period was extended after an intervention by the European Commission in the form of a state aid investigation. It was finally concluded that the project could not be financed solely on market conditions and required state aid, to which the Commission agreed under three conditions. Firstly, Paks II needed to be legally separated from the current owner of Paks 1, the MVM Group, so that losses could not be absorbed or hidden in the parent company. Secondly, there was a requirement to sell at least 30 per cent of its total electricity output on the open power exchange, with equal access to all market players. "The rest of Paks II's total electricity output will be sold by Paks II on objective, transparent and non-discriminatory terms by way of auctions", the Commission press release noted. The final condition stated that if the project was profitable, profits could not be reinvested for further developments, but only to pay the investment back to Hungary (Zalan, 2017).

Recent reports about renegotiations (Digges, 2019) and poorly explained changes to the project team (Hungary Today, 2019) have raised questions about other features of the contract, including the very nature of the arrangement that has been introduced to the public as a turnkey solution. The latter would entail that the NPP, when completed, would be handed over by the constructor to an owner operating independently and legally separated from the current owner, the MVM Group.

Interestingly, it seems that the contract has been classified for 30 years, citing national security reasons. Therefore, aspects that have been reported by various sources cannot be verified against the original text. An appeal court in Budapest has ruled that Rosatom and the Hungarian government have to declassify the agreements related to the upgrade of the Paks NPP (IntelliNews, 2019). No such agreements have been published as yet.

This differs significantly from the Hanhikivi case, where details of the project are publicly available and thus subject to public scrutiny. For instance, the Migrit Solarna case was one where the role of investigative journalism proved critical. Indeed, it stands as an example where a commitment to transparency allowed civil society to play the role of watchdog and spot suspicious activity that might have otherwise been overlooked.

Impacts

The intergovernmental agreement has clear benefits for both sides. Russia has used the project to support the modernisation of its economy and diversification of its export structure (Aalto, et al., 2017, p. 406). The Hungarian leaders do not see the Russian economic nexus as a substitute, but as a supplement to the Western one (Shentov, 2018, p. 148). The post-2010 Fidesz government has rolled back the privatisation achievements and effectively renationalised the energy sector, which has led to a reduction in the extent to which foreign companies of any origin influence the Hungarian energy sector (Ostrowski & Butler, 2018, p. 174). However, even if the Hungarian government is in control and can monitor foreign involvement, this does not preclude the government from finding itself in a position where it is subjected to pressure. An often-cited example of likely Russian influence was the decision in September 2014 whereby Hungary suspended reverse flow gas exports to Ukraine. This action came only three days after a high-level meeting between Hungarian and Russian officials, leading to accusations by observers that Russia must have wielded excessive influence over the Hungarian leadership, using them as a political pawn in its wider conflict with Ukraine (Ostrowski & Butler, 2018, p. 172). Moreover, a significant case in the gas sector between 2012 and 2015, which raised genuine concern about high-level collusion, if not corruption, between the Russians and the Hungarians was the MET gas trading scandal – a re-selling scheme, similar to a previous one in Ukraine, which benefitted one Russian and three Hungarian businessmen (Ostrowski & Butler, 2018, p. 173)

The Russian 10-billion-euro credit line for the Paks II project is roughly three times bigger than the highest estimates for Russian-related investments in Hungary as a whole. If Hungary utilises this credit line fully, it will create a direct government-to-government channel on a liability equal to 10% of the country's GDP. This will allow Russia to establish a self-supporting presence in the Hungarian energy sector and to extend it to other fields of the economy. (Shentov, 2018, p. 140).

A project of this magnitude will provide opportunities for Russian companies to establish further links in Hungary. There are concerns that the local contracts may not be subject to fair and transparent tenders, funnelling the lucrative contracts to the Hungarian oligarchs close to the government, citing the technical exclusivity exemption (Zalan, 2017) among other reasons. However, according to state aid rules, tenders to procure subcontractors should still be open (Zalan, 2017), a condition that the European Commission, based on past experience with this particular case, is highly likely to scrutinise.

The intervention by the EU structures proves the resilience of the internal market to foreign influence. The contract and business relations with Russia have been approved, while sending a very clear signal that the rules agreed in Brussels are not to be taken lightly. Despite the general defiance with regard to the EU, it appears that the situation has been advantageous for Hungary. All of the conditions have been beneficial for the EU as a whole, but Hungary has clearly benefitted the most.

Conclusion

It has been argued that social discourse on the extension of the Paks NPP, or nuclear power in general, is based on constructed realities, and that there is a lack of direct empirical evidence about the proceedings (Sarlós, 2015). Secrecy and classification add a special flavour to this construction. Several principal questions are unclear, starting from the terms of exit, payment schedule and other obligations of the parties. The Paks project is also a turnkey project, as are the Ostrovets and Hanhikivi NPPs. Differences in the perception of risk and benefit can be interpreted as an indicator of the lack of a commonly shared vision, and references to nuclear power are usually of a confrontational nature (Sarlós, 2015). All of this will potentially create distrust in the government and social division among the population.

In the case of Hungary, the NPP should be viewed in the wider context of energy policy and ties with Russia. Not only is Hungary dependent on Russia for its energy supply, but the current government has been able to stay in power partly owing to the Russian concessions in the energy sector. This includes the Gazprom concessions as well as the loan for the Paks project. The sitting government is not the only one to gain, as Russia also has its interests in play. As gas consumption in Hungary has decreased, the extension of Paks could be viewed as Russia's intent to maintain a grip on the Hungarian energy market in general, and drive the competition out by providing generous loans. This provides Russia with tools for priming (including corruption, blackmailing, and economic incentives) and various opportunities to use its economic leverage even for destabilisation. This might make Hungary particularly receptive and susceptible to hybrid activity. Some results of this could be seen in the cases of Hungary suspending reverse flow gas exports to Ukraine and the MET gas trading scandal. As in the Hanhikivi case, the EU dimension serves to connect the case to the wider Russian energy, foreign and security policy frame.

Observations about the Paks case study

- **Leverage that has been created through a business deal can also affect other agreements and domains. This was the case with the Hungarian decision to suspend the reverse flow of gas exports to Ukraine.**
- **An NPP can be used as leverage to create conflicts of interest and to hinder a robust response from the EU and NATO. Building a deterrence toolkit for hybrid threats should include mapping these kinds of potential leverages.**
- **The classification of business deals between states has the potential to undermine democracy and the rule of law. More work at the EU level should be done to prevent the spread of a culture of corruption.**
- **Energy diversification should not only entail different energy types, but also a variety of suppliers. The energy security of any country will be threatened if it is too dependent on one energy supplier. Even though Hungary has diversified in this respect, Russia is still its main energy provider.**

CONCLUSION: Nuclear energy and the potential creation of vulnerabilities for the future?

The objective of this report has been to explore risks related to civilian nuclear power in the contemporary security environment and in the context of hybrid threats. Compared to oil and gas politics, nuclear energy has received less attention as a potential tool for building influence and as leverage for exploiting vulnerabilities. Nuclear energy employed as a tool for any hostile intent has a different logic compared to oil and gas, for example, which have more explicit physical and logistical dependencies. Nuclear energy is still dependent on its distribution networks, which in this case are highly interconnected power grids that are also vulnerable to attack and manipulation. The EU has stated that its energy system is becoming increasingly integrated, while at the same time member states are importing from the same supplier countries. It is important therefore to consider energy security from an EU perspective, an issue that is reflected in the new Energy Article of the Lisbon Treaty. Choices made by one member state at the level of fuel supply, infrastructure development, energy transformation or consumption may lead to spill-over effects on other member states (European Commission, 2014). This report's findings support the Commission's view.

The report has also highlighted several points that can have potentially negative spill-over effects on other domains, which may increase the influence of the provider country over the decision-making of the client country, as well as the business culture and rule of law framework of client countries. A centralised building process can give rise to many vulnerabilities, most of which are related to economic leverage-building. In this report, all of the case studies used the Russian company Rosatom as their provider. The part of the report that takes a closer look at the latter makes a strong case for talking about the Russian state as the provider when talking about Rosatom. Building an NPP is a huge undertaking that not only involves engineering, construction, and the machining industry, but which also extends to other areas of the economy. Service arrangements, fuel supply and training obligations will allow Russia to establish a self-supporting presence in the energy sector, further advancing its existing interests and connections in hydrocarbons to nuclear energy and mutually reinforcing dependencies. Credit arrangements and negotiations over interest rates may also present a potential loophole for influencing political decisions in the future.

Moreover, NPP building projects also fall under geopolitical security. In historical terms, we know that building projects have been used for both intelligence-gathering and operations. From the point of view of hybrid threats, these types of projects provide an opportunity for priming, meaning that leverage can be exerted, the environment can be shaped, vulnerabilities can be exposed and created, and the capabilities of both the adversary and the target can be tested.

In all three case studies, it is possible to explain Rosatom's activities in commercial and competitive terms. Both sides, the buyer and the seller, have arguments to support their decision to engage with each other when the principal decision has been made in favour of nuclear energy. The large loans that the Russian state provides also have a commercial benefit. Compared with low interest rates and the volatile global environment, return on investment will be very stable for decades. There is also the remarkable spill-over effect of creating jobs in Russia. The symbiotic nature of the Russian state and one of its flagship industries creates a clear advantage over competitors when it comes to pricing, which seems to be challenging to overcome.

It is also possible to explain all of the case studies through Russia's strategic interests, which extend beyond business arguments. State veto

over business logic cannot be excluded. As James Henderson's examination of Rosatom in this report shows, there is certainly a political element involved. As one of only seven strategic "state corporations", the President of Russia appoints the company's Director General and members of the Supervisory Board, while the government approves the company's long-term strategy, and hence the management is clearly motivated to keep its political masters happy. The statements by the Russian high-level political elite also support the close relationship and cooperation argument. The risks relating to hybrid threats increase if the state in question, namely Russia, is at odds with the EU, NATO or with democratic principles in general.

The report examined risks stemming from the nuclear energy sector under the following headings: security of supply, economic leverage-building, nuclear proliferation and terrorism, the cyber domain, and information influence activities. Hypothetically speaking, if one NPP were targeted with tools from all of above-mentioned categories, a strong hybrid combination of tools would be created and the result would most likely be devastating.

The **security of supply** issue has tended to predominate when threats relating to nuclear energy have been discussed. Since nuclear energy reserves last longer in the event of supply disruptions compared to oil or gas, and alternatives can be found, the threat relating to security of supply has not usually been regarded as high. In the hybrid threat security environment, cuts or disruptions can be used to blur situational awareness, however. In this sense, if security of supply threats are used in combination with other activities, then they warrant taking seriously.

Economic leverage-building is a new old method, so to speak. It becomes a threat issue particularly when deals are made between democratic states and non-democratic states. Partners from less democratic political regimes are likely to challenge the normative environment and provoke changes in the business culture. Loans, supply dependencies, roles in the energy market, side deals and so forth all play a part in business, and are aspects that may be used by the state or by small interest groups to their own advantage while harming or undermining another party (Rosenkranz, 2006). Economic leverage-building may be a facet of priming, which is one of the phases of hybrid activity. Similarly to the security of supply issue, if we are talking about a business deal where proper risk assessments have been conducted, this alone does not increase the threat level. But as priming aims to bring about an effect over the long-term, seemingly straightforward economic aspects can turn into a serious weakness over time.

Nuclear proliferation and terrorism are closely interlinked with geopolitical security. As this heading indicates, nuclear energy can be used between states as a political and a politicised issue. In the case of oil and gas, the politicisation is usually associated with security of supply. Since the security of supply in terms of nuclear has a different mechanism compared to oil and gas, nuclear proliferation and terrorism are integral when talking about risks relating to nuclear energy. The dual-use capacity of the technologies and materials required to produce nuclear energy takes matters beyond the location and safety of an individual NPP. Moreover, unlawful nuclear programmes that are not observed by international organisations have been undertaken by non-democratic governments. This means that the polarisation of the international order between law-abiding states and rogue states increases the vulnerabilities in nuclear energy production as well, and makes it harder to control the dual use of nuclear energy material. Furthermore, an act of terrorism, if targeted against a nuclear facility or with nuclear materials (CBRN agents and technology), has far more serious consequences than acts against fossil fuels. An attack against an oil refinery, as in the case of Saudi Arabia, also has global implications, but nuclear energy disasters immediately put lives at risk and inflict harm in the long-term. Furthermore, the fact that NPPs are seen as strategically important facilities always brings the security political aspects into play. Such factors need to be taken particularly seriously when considering an NPP built in one country but very close to the border of another, as in the case of Ostrovets.

The cyber domain poses a new and real threat to the physical safety of NPPs. It is possible to attack NPPs covertly through cyber means, which could be a tempting option for terrorists, but also for states. Cyber attacks could create major power outages, and incite general fear and distrust around nuclear energy. This will be a major

future challenge and is a worrying development. The hybrid threat era has given rise to the notion of using attacks against NPPs as one of the tools in the adversarial hybrid threat toolkit. This is particularly relevant when it comes to intelligence-gathering. The continuously evolving cyber technology provides ever more sophisticated tools for conducting such operations. The cyber domain also poses new challenges for building projects as well as the running of power plants. The technical aspects are beyond the scope of this report, but note should be taken of the fact that cyber domain security planning needs to be examined through the hybrid threat lens.

Nuclear accidents and the devastation caused by them have made nuclear energy a very useful topic for **information influence activities**, a tool often used in the hybrid threat environment. Nuclear energy is clearly an issue that divides people and which can easily be used in information campaigns as a means of generating tensions in society, creating mistrust between government and civil society, and causing anxiety among the populace, in the hope that decisions in the target country will be made in a climate of fear. It is a well-known fact that fear compromises the ability to make pragmatic decisions. Nuclear energy is a form of energy production that carries major risks and hence it is important to have transparent and highly regulated and monitored safety rules. If these are not implemented, uncertainty will only exacerbate the fear surrounding nuclear energy.

This report has shown that nuclear energy as a tool merits further research from the hybrid threat perspective. If a nuclear energy aspect is added, in any form listed above, it will act as a strong force multiplier and strengthen the adversary's hand. Even if the direct risk of a nuclear accident is limited, spill-over to other domains constitutes considerable potential for interference and influence. The coincidence of Rosatom's business with key current and future allies of Russia in the global arena should be studied more closely. It is not entirely clear whether a nuclear energy deal is the result of existing good relations or should be seen as an investment for guaranteeing good relations in the future. All three case studies in this report indicate that the nuclear sector definitely warrants closer scrutiny and further security analysis. Since hybrid threats are ever-evolving, and adversarial actors, both state and non-state, have demonstrated the ability to think creatively and combine strategically, nuclear energy has to be seen as an important part of the hybrid threat landscape.

Aspects to consider

- **Nuclear energy and its role in energy dependencies should be studied more extensively, not least because all too often the focus has been on oil and gas. To this end, this report serves as an initial study on a highly complex issue. As hybrid threats are evolving and adversarial thinking is becoming more creative, potential threats related to nuclear energy should be included in training and exercise scenarios in order to counter and respond to them more effectively.**
- **Many of the hybrid threats relating to nuclear energy are not direct and obvious, but hidden and derive from spill-over effects. NPP building projects have embedded hybrid threat potential, where spill-overs to different domains such as intelligence, legal, economic, information, social, infrastructure, political and military can be used to create powerful leverage.**
- **Rosatom as an actor should be treated as a part of the Russian state's foreign policy. Any deal for NPP construction is strategic in nature and has other objectives aside from economic ones.**
- **Besides environmental and economic concerns, security and defence policy aspects should not be excluded from risk assessments of NPPs. NPPs are strategic assets and hence even military protection around them is possible, as the Ostrovets case study indicated. This protection could also be used offensively if a need or opportunity presents itself.**
- **Business communities as well as engineering/technical experts dealing with NPP safety issues should be educated about the landscape of hybrid threats.**
- **This report highlights the diversity of the threats related to nuclear energy and NPPs. Further work is required to assess the whole scale of risks relating to nuclear energy in the era of hybrid threats.**

Bibliography

Aalto, P., Nyyssönen, H., Kojo, M. & Pal, P., 2017. Russian nuclear energy diplomacy in Finland and Hungary. *Eurasian Geography and Economics*, 58(4), p. 406.

Balmaceda, M. M., 2014. *Living the High Life in Minsk: Russian Energy Rents, Domestic Populism and Belarus' Impending Crisis*. Budapest and New York: CEU Press.

BelTA, 2019. *Belarusian students getting on-the-job training at Rostov nuclear power plant*. [Online] Available at: https://eng.belta.by/society/view/belarusian-students-getting-on-the-job-training-at-rostov-nuclear-power-plant-118786-2019/ [Accessed 15 July 2019].

Cameron, G., 1999. *Nuclear Terrorism: A Threat Assessment for the 21st Century*. s.l.:Springer.

CCDCOE, 2019. *NATO Cooperative Cyber Defence Centre of Excellence home page*. [Online] Available at: https://ccdcoe.org/about-us/ [Accessed 20 June 2019].

De Clercq, G., 2017. *Rosatom would bid in Saudi Arabia nuclear plant tender*. [Online] Available at: https://www.reuters.com/article/saudi-nuclearpower-russia/refile-update-1-rosatom-would-bid-in-saudi-arabia-nuclear-plant-tender-idUSL8N1N880U [Accessed 8 August 2019].

Deak, A. & Amon, A., 2015. Hungary and Russia in economic terms – love, business, both or neither?. In: *Diverging voices, converging policies: the Visegrad states' reactions to the Russia-Ukraine conflict*. Prague and Warsaw: Heinrich Böll Stiftung.

Digges, C., 2019. *Hungary seeks to postpone loan payback to Russia for nuclear power plant: What will the final cost be?*. [Online] Available at: https://bellona.org/news/nuclear-issues/2019-02-hungary-seeks-to-postpone-loan-payback-to-russia-for-nuclear-power-plant-what-will-the-final-cost-be [Accessed 21 February 2019].

ENSEC COE, 2019. *NATO Energy Security Centre of Excellence homepage*. [Online] Available at: https://enseccoe.org/en/about/6 [Accessed 20 June 2019].

ENSREG, 2017. *NATIONAL REPORT OF THE REPUBLIC OF BELARUS ON THE BELARUSIAN NPP OBJECTIVE SAFETY REASSESSMENT (STRESS TESTS)*. [Online] Available at: http://www.ensreg.eu/sites/default/files/attachments/belarus_stress_test_national_report-31.10.2017_0.pdf [Accessed 15 July 2019].

ENSREG, 2018. *EU Peer Review Report of the Belarus Stress Tests*. [Online] Available at: http://www.ensreg.eu/sites/default/files/attachments/hlg_p2018-36_155_belarus_stress_test_peer_review_report_0.pdf [Accessed 8 August 2019].

Ercanbrack & Burmistrova, 2015. *Croatian investor in Finnish reactor has Russian-born owners*. [Online] Available at: https://www.reuters.com/article/us-fennovoima-nuclear/croatian-investor-in-finnish-reactor-has-russian-born-owners-idUSKCN0PH0WG20150707 [Accessed 15 July 2019].

ERR, 2019. *Kaliningrad successfully tests independent local electricity grid*. [Online] Available at: https://news.err.ee/945951/kaliningrad-successfully-tests-independent-local-electricity-grid [Accessed 8 August 2019].

Euratom Supply Agency, 2015. *Report on Nuclear Fuel Security of Supply.* [Online] Available at: http://ec.europa.eu/euratom/docs/2015-ESA-MEP-rapport-web.pdf [Accessed 22 June 2019].

European Commission, 2014. *European Energy Security Strategy.* [Online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0330&from=EN [Accessed 9 July 2019].

European Commission, 2014. *SWD(2014) 330 final: In-depth study of European Energy Security.* [Online] Available at: https://ec.europa.eu/energy/sites/ener/files/documents/20140528_energy_security_study_0.pdf [Accessed 5 August 2019].

Fennovoima, 2014. *Ydinvoimalaitoksen ympäristövaikutusten arviointiselostus.* [Online] Available at: https://www.fennovoima.fi/sites/default/files/media/documents/YVAselostus2014.pdf [Accessed 24 September 2019].

Fennovoima, 2018. *Story of Fennovoima.* [Online] Available at: https://www.fennovoima.fi/en/fennovoima/story-of-fennovoima [Accessed 15 July 2019].

Hillman, J. E., 2019. *Influence and Infrastructure: The Strategic Stakes of Foreign Projects.* [Online] Available at: https://csis-prod.s3.amazonaws.com/s3fs- public/publication/190123_Hillman_InfluenceandInfrastructure_WEB_v3.pdf [Accessed 1 July 2019].

Hukkanen, V., 2019. *Fennovoima ja voimalan toimittaja RAOS kertovat, miksi Pyhäjoen voimala on 10 vuotta myöhässä – "Kesällä mietittiin, jatketaanko vaiko ei".* [Online] Available at: https://yle.fi/uutiset/3-10589282 [Accessed 15 July 2019].

Hungary Today, 2019. *Paks Upgrade State Secretary Sacked.* [Online] Available at: https://hungarytoday.hu/paks-upgrade-state-secretary-sacked/ [Accessed 21 February 2019].

Hybrid CoE, 2019. *Hybrid CoE homepage.* [Online] Available at: https://www.hybridcoe.fi/what-is-hybrid-coe/ [Accessed 09 July 2019].

IAEA SEED Review Service, 2017. *Safety of the Belarusian NPP against Site Specific External Hazards.* [Online] Available at: https://www.iaea.org/sites/default/files/documents/review-missions/seed_mission_report_belarus_2017.pdf [Accessed 8 August 2019].

IAEA, 2017. *Country Nuclear Power Profiles: Belarus.* [Online] Available at: https://cnpp.iaea.org/countryprofiles/Belarus/Belarus.htm [Accessed 15 July 2019].

IAEA, 2017. *How Nuclear Power Helps Meet Global Energy Demand. The Role of the IAEA.* [Online] Available at: https://www.iaea.org/sites/default/files/18/04/how-nuclear-power-helps-meet-global-energy-demand-the-role-of-the-iaea-new.pdf [Accessed 21 June 2019].

IAEA, 2018. *Financing Nuclear Power in Evolving Electricity Markets.* [Online] Available at: https://www.iaea.org/sites/default/files/18/07/financing-np-0418.pdf [Accessed 8 August 2019].

IAEA, 2019. *PRIS - Power Reactor Information System.* [Online] Available at: https://pris.iaea.org/PRIS/home.aspx [Accessed 5 August 2019].

Iijama, J. & Hotta, T., 2019. *Hitachi reversal points to nuclear sector led by China and Russia.* [Online] Available at: https://asia.nikkei.com/Business/Companies/Hitachi-reversal-points-to-nuclear-sector-led-by-China-and-Russia [Accessed 15 July 2019].

Ilta-Sanomat, 2019. *Tutkija varoittaa Suomea: Pyhäjoen ydinvoimala mahdollistaa Venäjän salaiset operaatiot – "Loistava tekosyy".* [Online] Available at: https://www.is.fi/ulkomaat/art-2000006037478.html [Accessed 15 July 2019].

IMF, 2019. *IMF Country Report No. 19/9 REPUBLIC OF BELARUS.* [Online] Available at: https://www.imf.org/en/Publications/CR/Issues/2019/01/18/Republic-of-Belarus-2018-Article-IV-Consultation-Press-Release-Staff-Report-and-Statement-by-46526 [Accessed 8 August 2019].

IntelliNews, 2018. *Hungary's nuclear power plant expansion reportedly delayed.* [Online] Available at: https://www.intellinews.com/hungary-s-nuclear-power-plant-expansion-reportedly-delayed-151820/ [Accessed 22 February 2019].

IntelliNews, 2019. *https://www.intellinews.com/court-ruling-forces-hungarian-government-to-declassify-paks-upgrade-agreements-156179/.* [Online] [Accessed 22 February 2019].

Ioffe, G., 2018. *Belarusian Nuclear Power Plant Proceeding Full Speed Ahead.* [Online] Available at: https://jamestown.org/program/belarusian-nuclear-power-plant-proceeding-full-speed-ahead/ [Accessed 20 August 2019].

Johansson, B., 2013. A Broadened typology on energy security. *Energy*, Volume 53, pp. 199–205.

Kaleva, 2017. *Taloussanomat: Rosatom suunnittelee kesäksi lasten ydinvoimaleiriä Kalajoelle.* [Online] Available at: https://www.kaleva.fi/uutiset/kotimaa/taloussanomat-rosatom-suunnittelee-kesaksi-lasten-ydinvoimaleiria- kalajoelle/756040/ [Accessed 15 July 2019].

Katona, T. J., 2009. Future of the Nuclear Power Generation in Hungary [Online] Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/P1500_CD_Web/htm/pdf/topic1/1S06_T.J.%20Katona.pdf [Accessed 8 March 2019].

Kesler, B., 2011. The Vulnerability of Nuclear Facilities to Cyber Attack. *Strategic Insights*, 10(1), p. 17.

Kommersant, 2015. *"Росатом" нашел хорватских инвесторов: Они могут оказаться русскими.* [Online] Available at: https://www.kommersant.ru/doc/2758482 [Accessed 15 July 2019].

Lietuvos Republikos Seimas, 2017. *Law on recognition of the nuclear power plant under construction in the Ostrovets district in the Republic of Belarus as unsafe and posing a threat to the national security of the Republic of Lithuania, its environment and public health.* [Online] Available at: https://e-seimas.lrs.lt/rs/legalact/TAD/.../format/ISO_PDF/ [Accessed 15 July 2019].

Lithuanian MFA, 2018. *www.urm.lt.* [Online] Available at: statement-by-the-ministry-of-foreign-affairs-on-astravets-nuclear-power-%20plant-under-construction-in-belarus- [Accessed 15 July 2019].

Lough, J., 2011. *Russia's Energy Diplomacy.* [Online] Available at: https://www.chathamhouse.org/sites/files/chathamhouse/19352_0511bp_lough.pdf [Accessed 24 September 2019].

Martikainen, T. & Vihma, A., 2016. *Dividing the EU with energy?.* [Online] Available at: https://www.fiia.fi/wp-content/uploads/2017/10/bp191_dividing-the-eu-with-energy.pdf [Accessed 24 September 2019].

Mattlin, M. & Nojonen, M., 2011. *Conditionality in Chinese bilateral lending.* [Online] Available at: https://helda.helsinki.fi/bof/bitstream/handle/123456789/8282/168866.pdf?sequence=1&isAllowed=y [Accessed 8 August 2019].

McCurry, J., 2004. *South Korean nuclear operator hacked amid cyber-attack fears.* [Online] Available at: https://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack [Accessed 8 August 2019].

MCDC, 2019. *Countering hybrid warfare project.* [Online] Available at: https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare [Accessed 16 July 2019].

Meserve, J., 2007. *Sources: Staged cyber attack reveals vulnerability in power grid.* [Online] Available at: http://edition.cnn.com/2007/US/09/26/power.at.risk/ [Accessed 8 August 2019].

Miller , S. E. & Sagan, S. D., 2009. Nuclear power without nuclear proliferation?. *Dædalus, Journal of the American Academy of Arts and Sciences*, 138(4), pp. 7–18.

Minin, N. & Vlcek, T., 2017. Determinants and considerations of Rosatom's external strategy. *Energy Strategy Reviews*, September, Volume 17, pp. 1–2.

Ministry of Finance of the Russian Federation, 2019. *National Wealth Fund.* [Online] Available at: https://www.minfin.ru/en/key/nationalwealthfund/ [Accessed 15 July 2019].

Molden, D. C., 2014. Understanding priming effects in Social Psychology: What is "Social priming" and How does it occur?. *Social Cognition*, 32(Special Issue), pp. 1–11.

Morgan, S., 2017. *Belarus: Atomic power on the EU's doorstep.* [Online] Available at: https://www.euractiv.com/section/europe-s-east/news/belarus-atomic-power-on-the-eus-doorstep/ [Accessed 8 August 2019].

MVM, 2019. *Startpage - About Us.* [Online] Available at: http://www.atomeromu.hu/en/AboutUs/Lapok/1default.aspx [Accessed 15 July 2019].

Nurmi, L., 2018. [Online] Available at: https://www.aamulehti.fi/uutiset/presidentti-niinisto-fenno-voima-oli-varmasti-venajalle-hyvin-tarkea-kokosimme- yhteen-suomen-ja-venajan-suhteissa-kesalla-2015-tapahtuneet-kaanteet-201165922 [Accessed 15 July 2019].

Ostrowski, W. & Butler, E. eds., 2018. *Understanding Energy Security in Central and Eastern Europe.* s.l.: Routledge .

Ожаровский, А., 2016. Как «Росатом» спас Фенновойму [Online] Available at: https://bellona.ru/2016/05/11/fennovoima/ [Accessed 15 July 2019].

Oxenstierna, S., 2014. Nuclear Power in Russia's energy policies. In: S. Oxenstierna & V. Tynkkynen, eds. *Russian Energy and Security up to 2030.* Abingdon & New York: Routledge.

Oyserman, D. & Lee, S. W., 2008. Does Culture Influence What and How We Think? Effects of Priming Individualism and Collectivism. *Psychological Bulletin*, 134(2), pp. 311–342.

Palomaa, A., 2016. *Supo: Foreign intelligence sought to influence Finland's energy policy.* [Online] Available at: https://yle.fi/uutiset/3-8836171 [Accessed 15 July 2019].

Pamment, J., Nothhaft, H., Agardh-Twetman, H. & Fjällhed, A., 2018. *Countering Information Influence Activities: The State of the Art.* [Online] Available at: https://www.msb.se/RibData/Filer/pdf/28697.pdf [Accessed 8 August 2019].

Peel, M., 2017. *Lithuania given EU backing in nuclear plant dispute with Belarus.* [Online] Available at: https://www.ft.com/content/1cd6dc70-d137-11e7-b781-794ce08b24dc [Accessed 15 July 2019].

Песчинский, И., 2017. *Финская АЭС «Росатома» будет построена с опозданием.* [Online] Available at: https://www.vedomosti.ru/business/articles/2017/09/19/734375-finskaya-aes [Accessed 15 July 2019].

Preiherman, Y., 2018. *Belarus and Russia Resolve Their Pending Energy Issues, for Now.* [Online] Available at: https://jamestown.org/program/belarus-and-russia-resolve-their-pending-energy-issues-for-now/ [Accessed 5 September 2019].

Rosatom, 2018. *ROSATOM issues 2017 Annual Report.* [Online] Available at: https://www.rosatom.ru/en/press-centre/news/rosatom-issues-2017-annual-report/ [Accessed 24 September 2019].

Rosatom, 2019. *Akkuyu NPP: Major Milestone in Construction.* [Online] Available at: http://rosatomnewsletter.com/?post_turkey=akkuyu-npp-major-milestone-in-construction [Accessed 24 September 2019].

Rosenkranz, G., 2006. *Nuclear Power – Myth and Reality The risks and prospects of nuclear power.* [Online] Available at: https://www.boell.de/sites/default/files/assets/boell.de/images/download_de/ecology/NIP1RosenkranzEndf%28English_version%29.pdf [Accessed 24 September 2019].

Russian Government, 2015. *Энергетическая стратегия России на период до 2035 года [Russia›s energy strategy up to 2035].* [Online] Available at: http://www.energystrategy.ru/ab_ins/source/ES-2035_09_2015.pdf [Accessed 24 May 2017].

Sarlós, G., 2015. Risk perception and political alienism: Political discourse on the future of nuclear energy in Hungary. *Central European Journal of Communication*, 8(1(14)).

Schmid, J., 2019. The hybrid face of warfare in the 21st century. *Maanpuolustus*, March, pp. 12–17.

Schmitt, M. N. ed., 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge: Cambridge University Press.

Shentov, O., ed., 2018. *The Russian Economic Grip on Central and Eastern Europe.* s.l.:Routledge.

Sipola, T., 2017. *We turned on the radiation dosimeter and visited a relative of the notorious Chernobyl Nuclear Power Plant.* [Online] Available at: https://yle.fi/uutiset/3-9780666 [Accessed 8 August 2019].

Smok, V., 2016. *Belarus Struggles to Reduce Energy Dependence on Russia.* [Online] Available at: http://belarus-digest.com/story/belarus-struggles-to-reduce-energy-dependence-on-russia/ [Accessed 15 July 2019].

Soldatkin, V. & Nikolskaya, P., 2019. *Russia ready to take part in Bulgaria's Belene nuclear power plant: Prime Minister.* [Online] Available at: https://www.reuters.com/article/us-bulgaria-energy-nuclear-russia/russia-ready-to-take-part-in-bulgarias-belene-nuclear-power-plant-prime-minister-idUSKCN1QN1JB [Accessed 8 August 2019].

Stein, A., 2016. *Turkey's Nuclear Program – Challenges and Opportunities.* [Online] Available at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/AC-Turkey's%20Nuclear%20Program,%20Challenges%20and%20Opportunities.pdf [Accessed 24 September 2019].

Stratcom COE, 2019. *Hybrid Threats: A Strategic Communications Perspective.* [Online] Available at: https://www.stratcomcoe.org/download/file/fid/80212 [Accessed 15 July 2019].

Stratcom COE, 2019. *NATO Strategic Communications Centre of Excellence home page.* [Online] Available at: https://www.stratcomcoe.org/about-us [Accessed 20 June 2019].

STUK, 2011. *Vakavan ydinvoimalaturman aiheuttamat säteilyseuraukset.* [Online] Available at: https://www.julkari.fi/bitstream/handle/10024/123335/stuk-a228.pdf?sequence=1&isAllowed=y [Accessed 5 August 2019].

Česnakas, G. & Juozaitis, J., 2017. *Nuclear Geopolitics in the Baltic Sea Region: Exposing Russian Strategic Interests behind Ostrovets NPP.* [Online] Available at: https://css.ethz.ch/en/services/digital-library/articles/article.html/a15189ad-f30e-4c66-90df-d5d7c983a0da/pdf [Accessed 20 August 2019].

TEM, 2018. *FINLAND'S INTEGRATED NATIONAL ENERGY AND CLIMATE PLAN Draft version submitted to the European Commission.* [Online] Available at: https://tem.fi/documents/1410877/2132096/Suomen+NECP-luonnos+20.12.2018/318af23e-ad07-a984-7fcf-c439966306b7/Suomen+NECP-luonnos+20.12.2018.pdf [Accessed 15 July 2019].

Than, K., 2015. *Special Report: Inside Hungary's $10.8 billion nuclear deal with Russia.* [Online] Available at: https://www.reuters.com/article/us-russia-europe-hungary-specialreport/special-report-inside-hungarys-10-8- billion-nuclear-deal-with-russia-idUSKBN0MQ0MP20150330 [Accessed 12 March 2019].

Thomas, S., 2018. Russia's Nuclear Export Programme. *Energy Policy*, Volume 121, pp. 236-247.

Tiainen, O., 2017. *Totuus Fennovoiman kotimaisuusasteesta.* [Online] Available at: https://www.greenpeace.org/archive-finland/fi/media/blogi/totuus-fennovoiman-kotimaisuusasteesta/blog/58629/ [Accessed 8 August 2019].

Tikkala, H., 2015. *Fennovoima laskemassa rimaa – nyt riittää 60 prosentin eurooppalainen omistus.* [Online] Available at: https://yle.fi/uutiset/3-8067857 [Accessed 8 August 2019].

Tzanetakou, N., 2019. *Independent Balkan News Agency.* [Online] Available at: https://balkaneu.com/nuclear-power-plant-in-akkuyu-to-commence-operations-in-2023/ [Accessed 24 September 2019].

UK Energy Research Centre, 2009. *Building a resilient UK energy system*, London: UK Energy Research Centre.

UNECE, 2014. *Decision VI/2 Review of compliance with the Convention.* [Online] Available at: http://www.unece.org/fileadmin/DAM/env/eia/decisions/Decision_VI.2.pdf [Accessed 8 August 2019].

UNECE, 2018. *United Nations Economic Commission for Europe.* [Online] Available at: https://www.unece.org/fileadmin/DAM/env/pp/mop6/English/ECE_MP.PP_2017_2_Add.1_E.pdf [Accessed 8 August 2019].

UNECE, 2019. *Decision IS/1d on compliance by Belarus with its obligations under the Convention in respect of the Belarusian nuclear power plant in Ostrovets.* [Online] Available at: https://www.unece.org/fileadmin/DAM/env/eia/meetings/2019/IS_MOP_5-7_February_2019__Geneva/Decision_IS.1d_.pdf [Accessed 15 July 2019].

Uniter, 2012. *Oil refining industry outlook.* [Online] Available at: https://www.uniter.by/upload/overviews/Oil%20refining%20industry_outlook.pdf [Accessed 15 July 2019].

Verner, D., Grigas, A. & Petit, . F., 2019. *Assessing Energy Dependency in the Age of Hybrid Threats.* [Online] Available at: https://www.hybridcoe.fi/wp-content/uploads/2019/02/Assessing_Energy_Dependency_in_the_Age_of_Hybrid_Threats-HybridCoE.pdf [Accessed 20 June 2019].

Vijay, S., Hoikka, H. & Kenneth, B., 2017. *Cyber Warriors: course material.* [Online] Available at: https://mycourses.aalto.fi/pluginfile.php/457047/mod_folder/content/0/Cyber%20Warriors.pdf?forcedownload=1 [Accessed 15 July 2019].

Vlcek, T., 2016. Critical assessment of diversification of nuclear fuel for the operating VVER reactors in the EU. *Energy Strategy Reviews*, November, Volume 13–14, pp. 77–85.

Vuorikoski, S., 2019. *Eikä vieläkään Fennovoimaa.* [Online] Available at: https://suomenkuvalehti.fi/jutut/kotimaa/fennovoima-sponsoroi-pohjanmaan-painijoita-kalastajia-ja-hiihtajia-itse-ydinvoimala-yha-vailla-rakennuslupaa/ [Accessed 8 August 2019].

Ward, A., 2018. *Is the threat of nuclear terrorism distracting attention from more realistic threats?* [Online] Available at: https://www.weforum.org/agenda/2018/08/is-fear-of-nuclear-terrorism- distracting-us-from-more-realistic-threats/ [Accessed 1 July 2019].

Wesolowsky, T., 2016. *Belarus under fire for 'dangerous errors' at nuclear plant.* [Online] Available at: https://www.theguardian.com/world/2016/aug/09/belarus-under-fire-for-dangerous-errors-at-nuclear-plant [Accessed 8 August 2019].

WNA, 2011. *Ensuring Security Of Supply In The International Nuclear Fuel Cycle.* [Online] Available at: http://www.world-nuclear.org/uploadedFiles/org/WNA/Publications/Working_Group_Reports/security.pdf [Accessed 5 August 2019].

WNA, 2018. *Nuclear Power in the European Union.* [Online] Available at: https://www.world-nuclear.org/information-library/country-profiles/others/european-union.aspx [Accessed 8 August 2019].

WNA, 2019. *Nuclear Power in Belarus.* [Online] Available at: http://www.world-nuclear.org/information-library/country-profiles/countries-a-f/belarus.aspx [Accessed 15 July 2019].

WNA, 2019. *Nuclear Power in Finland.* [Online] Available at: https://www.world-nuclear.org/information-library/country-profiles/countries-a-f/finland.aspx [Accessed 8 August 2019].

WNA, 2019. *Nuclear Power in Hungary.* [Online] Available at: https://www.world-nuclear.org/information-library/country-profiles/countries-g-n/hungary.aspx [Accessed 5 August 2019].

WNN, 2016. *Belarus plant work suspended after installation mishap.* [Online] Available at: http://world-nuclear-news.org/NN-Belarus-plant-suspended-after-installation-mishap-02081601.html [Accessed 8 August 2019].

WNN, 2018. *Argentina, Russia expand nuclear energy cooperation.* [Online] Available at: http://world-nuclear-news.org/Articles/Argentina,-Russia-expand-nuclear-energy-cooperatio [Accessed 8 August 2019].

WNN, 2019. *Russia and Serbia to cooperate in nuclear power.* [Online] Available at: http://world-nuclear-news.org/Articles/Russia-and-Serbia-to-cooperate-in-nuclear-power [Accessed 8 August 2019].

WNN, 2019. *Turkey issues construction licence for Akkuyu unit 2.* [Online] Available at: http://world-nuclear-news.org/Articles/Turkey-issues-construction-licence-for-Akkuyu-unit [Accessed 24 September 2019].

World Bank, 2018. *Belarus - Country Partnership Framework.* [Online] Available at: documents.worldbank.org/curated/en/.../CPF-FY2018-22-Feb-21-03122018.docx [Accessed 8 August 2019].

YLE, 2018. *STUK remains concerned about Fennovoima's safety culture.* [Online] Available at: https://yle.fi/uutiset/3-10433691 [Accessed 15 July 2019].

Zalan, E., 2017. *EU gives green light to Hungary's nuclear plant.* [Online] Available at: https://euobserver.com/news/137122 [Accessed 6 March 2019].

Zetter, K., 2014. *An unprecedented look at Stuxnet, the world's first digital weapon.* [Online] Available at: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ [Accessed 8 August 2019].


Hybrid CoE