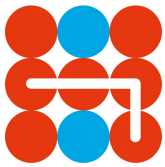
The European Centre of Excellence for Countering Hybrid Threats

Assessing Energy Dependency in the Age of Hybrid Threats

Duane Verner, Agnia Grigas, and Frederic Petit,
Energy and Global Security Directorate
Argonne National Laboratory

January 2019



Hybrid CoE

This report reflects the views of the authors only,
and does not necessarily represent the views of the U.S. government.

Contents

Introduction

Many nations including The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) member nations face significant challenges from hybrid threats involving the energy sector. The October 4, 2018, Federal Bureau of Investigation (FBI) indictments of Russians in the hacking of Westinghouse computer systems in Pittsburgh emphasizes the ongoing global nature of these challenges.[1] Halting Russian gas supply to Ukraine, on multiple occasions, has affected the gas supplies of European Union (EU) states, including during a cold 2008-2009 winter, which caused widespread hardship and contributed to casualties. These actions demonstrate the real risks of Russia's use of energy coercion. [2]

Therefore, enhancing the protection and resilience of member nations' energy systems is an urgent goal—a goal made more challenging by the inherent dependencies and interdependencies[3] within infrastructure systems and between energy-producing, -importing, and -transiting countries. Dependencies influence all components of risk: threat, vulnerability, resilience, and consequence. They can themselves be a threat, affect the resilience and protection of critical infrastructure, and lead to cascading and escalating failures. Growing dependencies across infrastructure systems, particularly reliance on information and communications technologies, have increased the potential vulnerabilities to physical and cyber threats and potential consequences resulting from the compromise of underlying systems or networks. In an increasingly interconnected world, where energy infrastructure crosses national borders and global supply chains, the potential impacts increase with these dependencies and the ability of adversaries to exploit them.[4] In addition, the geopolitics of energy, including global market and security considerations, is becoming more complex, which underscores the need to analyze and understand energy dependencies. Based on these factors, it is essential to integrate energy dependency considerations into hybrid threat, risk, and resilience assessments and strategies.

The goal of this paper is to enhance Hybrid CoE member nations' and allied organizations' understanding of energy dependencies in the context of today's hybrid threat security environment.

- Provides an overview of dependency-related policies and initiatives,
- Explains the geopolitics of energy dependencies,
- Describes the classes of dependencies, and
- Presents a general approach and recommendations for integrating energy dependency considerations into hybrid threat analysis and resilience assessments and strategies.

[1] Lynch, Sarah N., Lisa Lambert, and Christopher Bing (2018) "U.S. indicts Russians in hacking of nuclear company Westinghouse." Available at https://www.reuters.com/article/us-usa-russia-cyber/u-s-indicts-seven-russians-for-hacking-nuclear-company-westinghouse-idUSKCN1ME1U6. Accessed October 4, 2018.

[2] Harding, Luke, and Dan McLaughlin (2009) "Deal to resume Russian gas eludes EU as 11 people die in big freeze-up," Guardian, January 11. Available at https://www.theguardian.com/world/2009/jan/11/russia-ukraine-gas-supplies-dispute. Accessed October 4, 2018.

[3] A dependency is a unidirectional relationship between two assets or entities where the operations of one affect the operations of the other. An interdependency is a bidirectional relationship between two assets or entities where the operations of both affect each other. An interdependency is effectively a combination of two dependencies—therefore, understanding an interdependency requires analysis of the one-way dependencies that comprise it. (Source: Petit et al. [2015] Analysis of Critical Infrastructure Dependencies and Interdependencies, ANL/GSS-15/4, Argonne National Laboratory, Global Security Sciences Division, Argonne, Ill., USA. Available at http://www.ipd.anl.gov/anlpubs/2015/06/111906.pdf. Accessed October 3, 2018.)

[4] Petit, F., et al. (2015) Analysis of Critical Infrastructure Dependencies and Interdependencies, ANL/GSS-15/4, Argonne National Laboratory, Global Security Sciences Division, Argonne, Ill, USA. Available at https://publications.anl.gov/anlpubs/2015/06/111906.pdf. Accessed September 28, 2018.

Dependency-Related Policies and Initiatives

The definition, classification, protection, and resilience of critical infrastructure traditionally comprise a national competency. For example, in the United States, Presidential Policy Directive 21 (PPD-21) and the National Infrastructure Protection Plan (NIPP) guide the strategy for enhancing the protection and resilience of critical infrastructure. PPD-21 establishes the need for operational and strategic analysis to identify infrastructure dependencies and to incorporate them into risk assessment and management procedures.[5] The 2013 edition of the NIPP reinforces the need to understand and address risks from cross-sector dependencies to enhance infrastructure security and resilience. [6]

The need for strategic risk analysis of critical infrastructure dependencies is also a regional and global consideration. A Joint Declaration between the United States and Poland on Energy Security, signed in September 2018, emphasizes the need to address energy dependency-related challenges facing Poland as well as the broader international community. The Declaration promotes the development of the infrastructure necessary to increase regional energy security and diversification of sources and promotes the need to counter projects driven by malign actors, which use energy as a means of political and economic coercion. [7]

Energy infrastructure systems are highly interconnected. For example, Figure 1 shows the interdependencies associated with the electricity subsector. Although such interdependence has significantly benefited society in terms of efficiency, it can be a weakness when the failure or exploitation of interdependent systems generates cascading and escalating effects. As highlighted in the 2013 NIPP, "growing [dependencies and] interdependencies across critical infrastructure systems, particularly reliance on information and communications technologies, have increased the potential vulnerabilities to physical and cyber threats and potential consequences resulting from the compromise of underlying systems or networks. In an increasingly interconnected world, where critical infrastructure crosses national borders and global supply chains, the potential impacts increase with these [dependencies and] interdependencies and the ability of a diverse set of threats to exploit them." [8]

The following pages present recent dependency-related policies and initiatives by region or international organization.

[5] The White House (2013) Presidential Policy Directive 21: Critical Infrastructure Security and Resilience. Available at https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf. Accessed September 28, 2018.

[6] DHS (2013) National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience. Available at https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf. Accessed September 28, 2018.

[7] DOE (2018) Joint Declaration between the United States Department of Energy and the Ministry of Energy of the Republic of Poland Concerning Enhanced Cooperation On Energy Security. Available at https://www.energy.gov/sites/prod/files/2018/11/f57/US-Poland%20Declaration%20for%20Enhanced%20Cooperation%20on%20Energy%20Security.pdf. Accessed January 2, 2019.

[8] DHS (2013) National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience. Available at https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf. Accessed September 28, 2018.

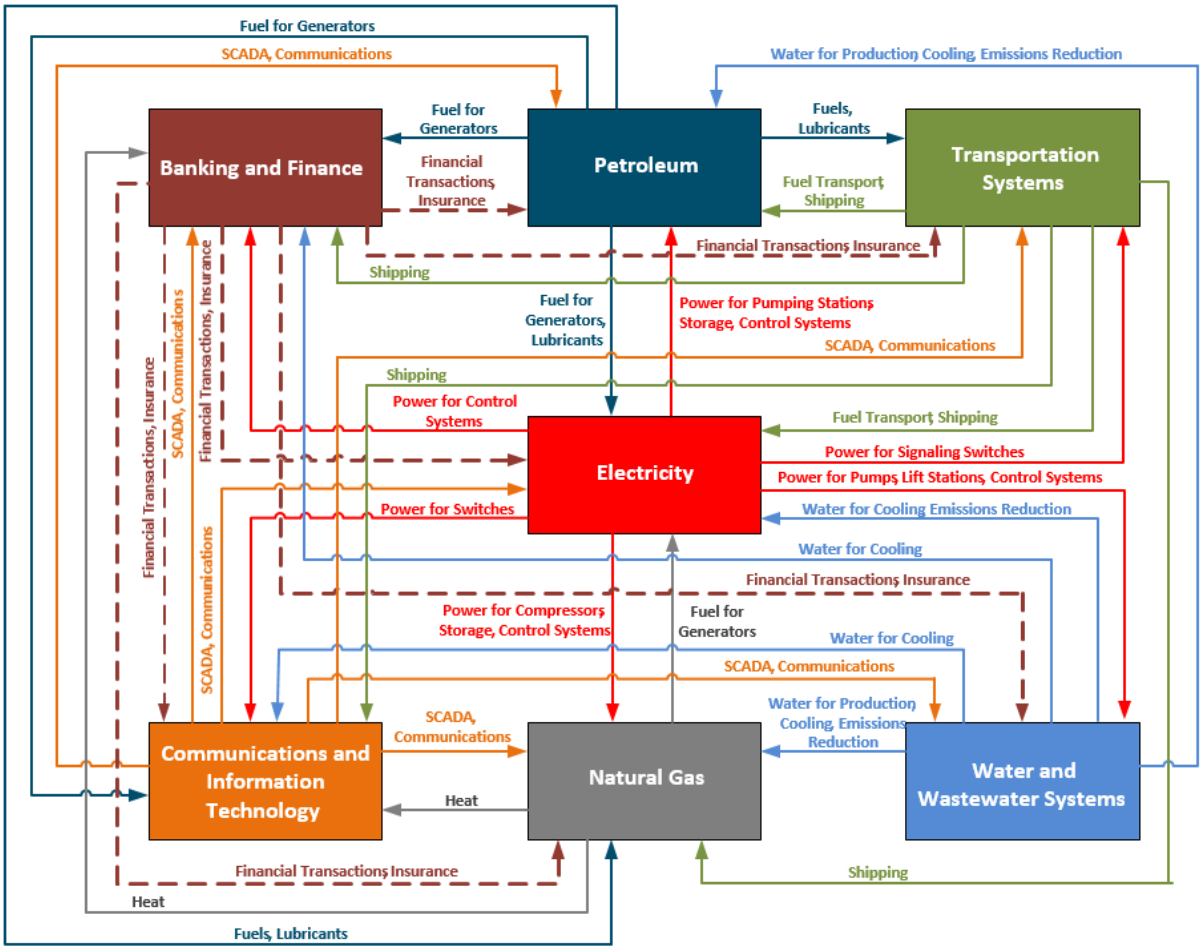


Figure 1: Electricity Interdependencies[9]

[9]Source: Argonne National Laboratory

North America

Following the Northeast blackout in 2003, the U.S. and Canadian governments created a task force to analyze the causes and make recommendations to prevent or mitigate future disruptions.[10] Since the work of this task force, plans and strategies developed between the United States and Canada have reiterated the importance of considering dependencies in risk-management processes.

The Canada-United States Action Plan for Critical Infrastructure, in particular, presents a cross-border approach to strengthening the resiliency of critical infrastructure. One of the three objectives of this action plan is to develop a collaborative risk-management approach, which requires identifying and addressing key infrastructure.[11] The Joint United States-Canada Electric Grid Security and Resilience Strategy identifies the need to integrate infrastructure dependency considerations to ensure the security and resilience of the electric grid. One of the main goals of this strategy is specifically to "understand and mitigate vulnerabilities from dependencies with other critical infrastructure."[12]

Europe

Concerns about critical infrastructure protection began in the late twentieth century in relation to tensions resulting from the Cold War. After the fall of the Eastern bloc, these concerns faded, only to resurface at the dawn of 2000 because of computer problems anticipated for the new millennium. This need to analyze and protect critical infrastructure has grown with respect to fears of terrorism, which have increased over the past 15 years, from the terrorist attacks of September 11, 2001, in the United States, to the upsurge of terrorism-related events in Europe in 2016 and 2017.

Similar to North America, the EU developed specific supranational programs for the protection of critical infrastructure. In December 2004, the Commission established a European Program for Critical Infrastructure Protection (EPCIP) and a warning system for critical infrastructure, the Critical Infrastructure Warning Information Network (CIWIN).[13] The objectives of EPCIP were to ensure adequate and uniform levels of safety for critical infrastructure, to minimize disruption, and to provide rapid reaction capabilities.[14] CIWIN allows for the exchange of best practices by providing a means of transmitting alerts and threat information.[15]

The EU is highly dependent on energy importation. This dependence leaves member nations vulnerable to supply disruptions. To address this concern, The European Commission defined its Energy Security Strategy to ensure a stable and abundant supply of energy for European citizens and the economy. The strategy specifically included short-term and long-term measures. Energy security stress tests led to the development of security preparedness plans. Long-term measures seek to promote more coordination between EU countries to use existing storage facilities, develop reverse flows, construct energy interconnectors, conduct risk assessments, and establish security-of-supply plans at the regional and EU levels.[16]

United Nations (UN)

UN Resolution 2341, dated February 2017, addresses threats to international peace and security caused by terrorist acts. The resolution specifically recognizes that the increase in

[10] U.S.-Canada Power System Outage Task Force.2004. Final report on the August 14, 2003, blackout in the United States and Canada: causes and recommendations. Available at https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf. Accessed September 28, 2018.

[11] Public Safety Canada (2010) Canada-United States Action Plan for Critical Infrastructure. Available at https://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf. Accessed September 28, 2018.

[12] Governments of the United States and Canada (2016) Joint United States–Canada Electric Grid Security and Resilience Strategy, December. Available at https://www.nrcan.gc.ca/sites/www.nrcan.gc.ca/files/energy/pdf/JOINT%20GRID%20SECURITY%20AND%20RESILIENCE-Strategy_en.pdf. Accessed September 28, 2018.

[13] Europa (2012) European Programme for Critical Infrastructure Protection. Available at http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm. Accessed September 28, 2018.

[14] Commission of the European Communities (2006) European Programme for Critical Infrastructure Protection, 576 final, Brussels, Belgium. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33260. Accessed September 28, 2018.

[15] Ibid.

[16] Europa (2018) Energy Security Strategy. Available at https://ec.europa.eu/energy/en/topics/energy-strategy-and-energy-union/energy-security-strategy. Accessed September 28, 2018.

cross-border critical infrastructure interdependencies between countries—combined with increasing threats and vulnerabilities—creates new security concerns.[17] The protection of critical infrastructure, therefore, requires an all-hazard approach promoting information sharing among governmental authorities, foreign partners, and the private sector, as well as domestic and cross-border collaborations to develop policies, good practices, and lessons learned.[18]

North Atlantic Treaty Organization (NATO)

Enhancing the resilience of critical infrastructure is a top priority for NATO, which complements the collective defense clause in Article 5. NATO has a significant dependency on civil and commercial infrastructure, including military transport, communications used for defense purposes, and host nation support to NATO operations from local commercial infrastructure and services. Many of these dependencies lack redundancies,[19] highlighting the need to identify and mitigate potential failure points vulnerable to exploitation through hybrid interference and influencing.

Specific to energy, the 2018 Brussels Summit Declaration states: "… it is essential to ensure that the members of the Alliance are not vulnerable to political or coercive manipulation of energy, which constitutes a potential threat." Because many NATO allies depend on Russian gas and oil, the resiliency of energy infrastructure plays an especially critical role in the common security of NATO member nations. Therefore, identifying stable and reliable energy supplies, diversifying transport routes, establishing suppliers and energy resources, and understanding the interdependencies within energy networks are vitally important to increasing resilience against hybrid threats.[20]

NATO is enhancing the resilience of critical infrastructure by improving situational awareness, strengthening deterrence and defense, and expanding its toolset to address hostile hybrid operations.[21] At the 2016 Summit in Warsaw, Allied leaders committed to further developing their nations' individual and collective capacity to resist any form of attack, including hybrid warfare; assist an ally that is a target in a hybrid operation; and counter hybrid warfare as part of a collective defense.[22] The 2018 Brussels Summit Declaration announced the establishment of Counter Hybrid Support Teams, which provide targeted assistance to Allies in preparing for and responding to hybrid operations. The Declaration also identified support for Ukraine's efforts to strengthen its resilience against hybrid threats by intensifying activities under the NATO-Ukraine Platform on Countering Hybrid Warfare.[23]

Other International Organizations

Other intergovernmental organizations, such as the World Economic Forum (WEF) and the Organisation for Economic Co-operation and Development (OECD), identify the importance of assessing infrastructure interdependencies. OECD specifically highlights the importance of understanding the characteristics of complex systems in anticipating catastrophic events that could result in global shocks.[24] The WEF's 2013 Global Risk Report also highlighted the need to consider interdependencies and prioritize appropriate response measures.[25] These two organizations are particularly interested in anticipating events that may require policy interventions and identifying where those interventions should or could occur.[26,27]

[17] United Nations Security Council (2017) "Resolution 2341: Threats to international peace and security caused by terrorist acts," February 13. Available at http://unscr.com/en/resolutions/doc/2341. Accessed September 28, 2018.

[18] Ibid.

[19] NATO (2018) "Resilience and Article 3." Available at https://www.nato.int/cps/en/natohq/topics_132722.htm. Accessed September 28, 2018.

[20] NATO (2018) "Brussels Summit Declaration," July 11–12. Available at https://www.nato.int/cps/en/natohq/official_texts_156624.htm. Accessed September 30, 2018.

[21] Ibid.

[22] Ibid.

[23] Ibid.

[24] OECD (2011) Future Global Shocks: Improving Risk Governance. Available at http://www.oecd.org/governance/48329024.pdf. Accessed September 28, 2018.

[25] WEF (2013) Global Risks 2013, Eighth Edition. Available at http://reports.weforum.org/global-risks-2013/. Accessed September 28, 2018.

[26] Ibid.

[27] OECD (2011) Future Global Shocks: Improving Risk Governance. Available at http://www.oecd.org/governance/48329024.pdf. Accessed September 28, 2018.

Critical infrastructure dependency analysis can take various forms. National governments and critical infrastructure operators are responsible for the protection and resilience of critical infrastructure systems; their responsibilities require an operational approach. Supranational organizations, like the UN and NATO, have a coordination role and propose strategic approaches to promote the integration of national programs. Challenges addressed through these approaches must include the exploitation of dependencies through hybrid threats. Tailoring the approaches to consider hybrid operations requires consideration of geopolitics, infrastructure systems, and assets that comprise energy dependencies.

Geopolitics of Energy Dependencies

Because energy trade is highly political, it is useful to examine the geopolitical aspects of energy dependencies in assessing risk. Such dependencies reflect the geopolitical, political, and commercial relationships among three categories of nations: those that produce energy, those that import energy, and those whose territories or territorial waters are essential for the flow of energy supplies from producing to importing nations (transiting countries). When assessing the factors that influence the geopolitics of energy dependencies, researchers need to consider the distinctions between different resources, such as natural gas, oil, coal, nuclear, or renewables. Fungible commodities (those that can be easily exchanged or replaced) are less susceptible to politics because they are easy to transport and their global market and trade mechanisms are more robust. Less fungible resources tend to be more highly politicized and therefore more vulnerable to geopolitics. None of the categories described below is mutually exclusive; often, researchers can evaluate a country across multiple categories, depending on the circumstances.

Politics of Interdependence

While the term "energy politics" implies an element of power and influence, the relationships are complex and not one-sided. Exporting nations depend on their markets or on importing nation(s) for revenue. The resulting relationship can be one of interdependence or one of varying degrees of dependence, resulting in stable supplies that are less vulnerable to political shifts. The degree of interdependence varies depending on a number of conditions, such as the balance (or symmetry) in the dependency relationship between a supplier and a consumer, which reflects (1) the size of both markets, (2) the degree to which each side has alternative import or export market opportunities, and (3) related infrastructure. The degree of symmetry is not static: it can change with changing market conditions; discoveries of new resources or technologies; economic performance; and other domestic, bilateral, and international factors. In the real world of trade and commercial relations, perfectly balanced interdependence is rare.

Politics of Supply

When the balance of the relationship between the supplier and importer nations is tilted in favor of the supplier, that nation can pursue a set of policies known as the "politics of supply," negotiating from its position of strength relative to the consumer nation. Supplier nations can also advance their national, economic, political, and security interests by implementing certain economic and political policies: flooding or starving the market, favoring allies, or punishing enemies by implementing pricing or supply policies. For instance, negotiations of gas supplies or prices can be accompanied by demands that importing nations alter their domestic or foreign policies and/or join political or economic blocs or alliances with the supplier nations rather than rival ones.

Not all gas-producing countries can pursue the politics of supply. Certain characteristics can either constrain or broaden its power and influence in the supply relationship. Smaller suppliers that cannot meet a significant portion of their customer nation's needs lack the market or political leverage over importers. Likewise, regionally isolated suppliers who cannot access many markets or importing countries are much weaker players in the politics of supply.

Politics of Dependence

When the interdependence of suppliers and importing nations is asymmetric, the importing countries can fall prey to the "politics of dependence" or the "politics of demand," depending on their level of diversification, volume of imports, and market conditions. Such importers are disproportionately reliant on a single or limited set of energy-producing or -exporting nation(s), supply routes, or infrastructure. With limited political and economic options available, they often operate from a position of weakness.

Politics of Demand

In contrast, the "politics of demand" is a set of economic and political policy options available to energy-consuming countries to pursue their national economic, political, and security interests

by leveraging their strong position in energy markets or relative to specific gas-exporting countries or sets of countries. For instance, an importing country can enjoy a position of strength and negotiation leverage simply because it imports large volumes of a commodity or by having a number of diversified suppliers. The difference between being stuck in the politics of demand versus benefiting from the politics of supply can also depend on market conditions, such as liquidity and pricing, which determine whether it is a buyer's or seller's market.

Politics of Transit

The term "politics of transit" describes the dynamics for transit states, which retain some negotiating power by collecting revenues in the form of transit fees or for operating energy transit infrastructure; however, these nations can also fall into the trap of being "rentier states." Transit countries can use energy supplies as a means of coercion by destabilizing the transport of commodities through their territory, essentially holding supplies hostage. Historically, transit states have relied on land-based pipelines or rail or truck deliveries, but the boom of tankers carrying oil and liquefied natural gas (LNG) across global markets has added the element of international waters to the equation. [28]

[28] For a detailed analysis of the geopolitical dependencies described in this section, see Grigas, Agnia (2017) The New Geopolitics of Natural Gas, Harvard University Press, Cambridge, MA, p. 13–20.

Classes of Dependencies

Critical infrastructure assets are in constant interaction with their socio-economic environment, using and transforming inputs (i.e., resources) from the environment and providing outputs (i.e., new resources) to the same environment (e.g., other critical infrastructure assets). Several characteristics of the critical infrastructure considered and its operating environment (e.g., policy, security, safety, political considerations) have specific effects on the interconnections among critical infrastructure assets.[29] The best method by which to characterize critical infrastructure dependencies is to consider their classes based on the types of resources transferred and the level of interaction:[30,31]

Physical

This class of dependency characterizes the functional and structural linkages required to transfer goods and services. The connections (i.e., pipelines) between the natural gas system and the electric power system that supply the natural gas needed to fire up thermal generating plants constitute physical dependencies.

Cyber

This class of dependency characterizes the electronic and informational linkages required to transfer information and data. The transfer of data between sensors and the control center for monitoring day-to-day pipeline operations constitutes a cyber-dependency.

Geographic

This class of dependency characterizes the collocation of infrastructures and the potential that the disruption of one infrastructure asset may affect other infrastructure assets located nearby. The collocation of natural gas pipes and underground electric lines in urban right-of-ways constitutes a geographic dependency.

Logical

This class of dependency characterizes linkages attributable to human and financial decisions and actions. Geopolitical and financial decisions influencing the availability and the price of natural gas constitute logical dependencies.

Geographic dependencies define major energy corridors. Physical and cyber dependencies occur at operational and control levels. Finally, logical dependencies occur at management and strategic levels. All these classes of dependencies directly affect the energy supply chains. Their consideration in risk management and resilience strategies is important to understand the functioning of energy systems and to anticipate potential cascading and escalating failures resulting from hybrid threats.

The following section provides historical examples of interdependence among energy subsectors.

[29] Rinaldi, S.M., J.P. Peerenboom, and T.K. Kelly (2001) "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," IEEE Control Systems Magazine, December. Available at https://ieeexplore.ieee.org/document/969131. Accessed September 28, 2018.

[30] Ibid.

[31] Petit, F., et al. (2015) Analysis of Critical Infrastructure Dependencies and Interdependencies, ANL/GSS-15/4, Argonne National Laboratory, Global Security Sciences Division, Argonne, Ill, USA. Available at https://publications.anl.gov/anlpubs/2015/06/111906.pdf. Accessed September 28, 2018.

Case Studies

European Union and Gazprom

The energy relationship between Europe and Russia has been one of asymmetric energy interdependence. The EU has imported Russian oil and natural gas, while Russia has historically depended on European markets, as well as European investments and technologies. However, the EU has faced the politics of dependence in the gas sector, where Russian gas represented up to 40 percent of its gas imports.[32] Individual EU nations reflect a wide spectrum of energy security risks based on their relative (in)dependence from Gazprom—the largest supplier of natural gas to Europe and Turkey— complicating efforts to develop a common approach in Brussels.

According to Agnia Grigas' book, The New Geopolitics of Natural Gas, although Moscow employed gas cutoffs in the former Soviet Union during the 1990s as a well-established pressure tactic, several flashpoints in the 2000s contributed to a reevaluation of the EU's perception of Russia as a reliable gas supplier and marked a new stage in EU-Russia gas relations. In the winters of 2006 and 2009, Russia ceased supplies to Ukraine over tensions between Gazprom and Kyiv over gas prices. The dispute halted Russian gas deliveries to the EU that were transiting through pipelines on Ukrainian territory. The 2009 gas crisis lasted 2 weeks and affected supplies to the following EU member states: Czech Republic, Romania, Austria, Poland, Croatia, and Slovakia. The halt in gas supplies resulted in at least 11 casualties as citizens froze to death, including 10 people in Poland, where temperatures reached negative 20 degrees Celsius.[33]

After its purported annexation of Crimea and continued aggression in eastern Ukraine, Russia dramatically increased the price of gas sold to Ukraine. In June 2014, when Kyiv refused to pay for gas at the inflated rate for several months, Russia cut off supplies. Subsequently Ukraine has been receiving Russian gas in reverse flows from its European neighbors rather than from Russia directly.[34] Nonetheless, in March 2018, despite the Stockholm Arbitration panel, Gazprom refused to resume gas shipments to the Ukrainian market, forcing Kyiv to suspend schools and universities during the winter months and creating risks to the EU's supply.[35]

Going forward, the risks associated with Europe's dependence on Russian gas remain; the least severe of these risks could include price hikes and cutoffs. The EU's vulnerability to gas cutoffs will increase with the construction of the Gazprom-led Nord Stream 2 natural gas pipeline, which will concentrate two-thirds of Russian gas exports to Europe in parallel interconnectors (Nord Stream 1 and Nord Stream 2). Europe could not survive even 30 days without Russian gas in the winter, while Russia can certainly survive a year (if not years) without European gas purchases, investments, and technologies.[36] This situation will prove dire when Russia's Power of Siberia gas pipeline to China becomes operational in late 2019 and Russia obtains alternatives to European markets. As a result, the Kremlin may apply a carrot-and-stick approach to the EU and individual member nations and seek to sway both their domestic and foreign policies in relation to gas trade.

Nordic-Baltic Region: Power & Pipelines

The Nordic-Baltic region faces a number of risks related to new energy infrastructure projects, led

[32] Keating, Dave (2018) "While Expelling Diplomats, Germany Quietly Increases Dependence on Russian Gas," Forbes, March 29. Available at https://www.forbes.com/sites/davekeating/2018/03/29/while-expelling-diplomats-germany-quietly-increases-dependence-on-russian-gas/#5c340f955b1c. Accessed October 6, 2018.

[33] Harding, Luke, and Dan McLaughlin (2009) "Deal to resume Russian gas eludes EU as 11 people die in big freeze-up," Guardian, January 11. Available at https://www.theguardian.com/world/2009/jan/11/russia-ukraine-gas-supplies-dispute. Accessed October 6, 2018.

[34] For a historical overview of EU-Russia gas relations, see Grigas, Agnia (2017) The New Geopolitics of Natural Gas, Harvard University Press, Cambridge, MA, p. 146–161.

[35] Soldatkin, Vladimir, and Natalia Zinets (2018) "Gazprom seeks to halt Ukraine gas contracts as dispute escalates," Reuters, March 2. Available at https://www.reuters.com/article/us-russia-ukraine-gas/gazprom-seeks-to-halt-ukraine-gas-contracts-as-dispute-escalates-idUSKCN1GE2DW. Accessed October 6, 2018.

[36] Umbach, Frank (2014) "Russian-Ukrainian-EU gas conflict: who stands to lose most?" ***NATO Review***. Available at https://www.nato.int/docu/review/2014/nato-energy-security-running-on-empty/Ukrainian-conflict-Russia-annexation-of-Crimea/EN/index.htm. Accessed October 1, 2018.

by both the EU and Russia. The EU member states seek to diversify their sources of energy, as with the NordBalt power cable, and Russian energy companies seek to increase access to EU markets, as with the Nord Stream 2 pipeline. These new projects demonstrate the geopolitical factors that make up the politics of dependence, as well as physical, cyber, geographic, and logical dependency classes.

NordBalt, the submarine power cable between Lithuania and Sweden, expands integration of the Baltic states to the Nordic electricity markets and facilitates power trading between the Baltic and Nordic states. Geographic dependency risks could be a significant consideration for the power cable in the future. The Baltic Sea is a small, flat body of water—less than 20 meters deep in some places—and littered with countless mines, unexploded bombs, and sunken vessels from the two world wars. Accidental explosions are a real concern: in 2015, part of the Nord Stream 1 pipeline was briefly closed after the Swedish navy discovered an unexploded mine nearby. Moreover, Russia could also pose a security threat to Baltic energy infrastructure. Despite its small size, the Baltic Sea is home to a significant amount of Russian military activity, including large-scale exercises and regular patrol missions. Over the years, Russian servicemen have caused numerous high-risk incidents against NATO forces, including in the Baltic Sea.[37]

With Nord Stream 2, Russia intends to expand the infrastructure delivering gas directly to Germany under the Baltic Sea, bypassing Ukraine as a transit state and depriving it of $3 billion in annual transit revenues (roughly equivalent to Ukraine's Ministry of Defense budget in 2018).[38,39] While Nord Stream 2 would face the same risks of explosions or accidental military accidents as NordBalt in the Baltic Sea, if built, the new pipeline would increase Europe's vulnerability to a cutoff of gas supplies because it will concentrate two-thirds of Russian gas imports along the same route. The pipeline would also remove a key strategic deterrent against Russian aggression in Ukraine without fear of damage to the gas infrastructure that supplies European markets. It would also give Moscow new means of using energy for political coercion in Ukraine and in Europe more broadly.

Finally, the new pipeline would not only facilitate Russia's export of corruption to European business and politics but also increase the susceptibility of the EU's gas supply to cyber risks. There are major drawbacks to concentrating EU's pipeline infrastructure, as Nord Stream plans to do. Given that Nord Stream AG will operate both Nord Stream 1 and 2, the pipelines will likely have overlapping software that monitors day-to-day operations, and, at the exit, the two pipelines will be joined with interconnected hardware. Therefore, if hackers wanted to gain access to both pipelines, they would only have to hack into one system, not two, putting between one-third and one-fourth of EU gas imports at risk.

Ukraine and Nuclear Manipulation

While the Kremlin is best known for using natural gas for political advantage, Russia and its national nuclear energy company, Rosatom, have also vied for dominance in nuclear energy. A large number of EU and NATO countries are dependent on Russian-built nuclear power plants for their electricity; Moscow could use this dependence as a coercive tool, creating a long-term strategic vulnerability for ally states.

In late 2014, when the conflict between Kyiv and Moscow escalated, Ukraine decided to purchase nuclear fuel from the U.S. nuclear engineering group and global leader in nuclear fuel production, Westinghouse.[40] Its traditional supplier, Rosatom, previously had a near monopoly in the Ukrainian market. The Kremlin launched a propaganda and disinformation campaign. The Russian Foreign Ministry issued a statement, which was widely promoted on Russian media, that Ukraine was endangering public safety in Europe by using a U.S. supplier for Soviet-built nuclear plants.

[37] Grigas, Agnia, and Lukas Trakimavicius (2018) "Nord Stream 2 is a Bad Deal for Europe," Atlantic Council, July 10. Available at http://www.atlanticcouncil.org/blogs/new-atlanticist/nord-stream-2-is-a-bad-deal-for-europe. Accessed October 6, 2018.

[38] Carrel, Paul, and Madeline Chambers (2018) "Merkel says Nord Stream 2 not possible without clarity for Ukraine," Reuters, April 10. Available at https://af.reuters.com/article/worldNews/idAFKBN1HH1HP. Accessed October 10, 2018.

[39] Defense Express (2018) "Ukraine's Ministry of Defense 2018 budget approved at $3.1B," March 26. Available at https://defence-ua.com/index.php/en/news/4345-ukraine-s-ministry-of-defense-2018-budget-approved-at-3-1b. Accessed October 10, 2018.

[40] Williams, Carol J. (2014) "Russia says Ukraine deal to buy U.S. nuclear fuel poses safety risks," Los Angeles Times, Dec. 30. Available at http://www.latimes.com/world/europe/la-fg-russia-ukraine-nuclear-fuel-20141230-story.html. Accessed October 5, 2018.

They noted: "Consequences of possible accidents and meltdowns will be the full responsibility of the Ukrainian authorities and U.S. suppliers of the fuel." The statement referenced the world's worst nuclear disaster, the 1986 Chernobyl meltdown in Soviet-run Ukraine: "It seems that the Chernobyl tragedy did not teach Kyiv authorities any lessons." This panic-inducing statement from the Russian Foreign Ministry did not reflect the fact that Westinghouse had been working in the Ukrainian market since 2003, including operation of the South Ukraine Nuclear Power Plant.

The Kremlin has tried to stoke anxiety in the Ukrainian public, which continues to suffer the consequences of Chernobyl. Web blogs ran stories like this one from January 12, 2015, "Oh no! Kiev plans to jam (nuclear) square pegs into round holes."[41] Given that nuclear energy is responsible for 60 percent of electricity generation in Ukraine, supplies to nuclear power plants are of strategic domestic economic and political importance.[42] With Kyiv having faced a number of Gazprom gas cutoffs, a turn to Westinghouse during times of tension with Moscow could be perceived as a means of ensuring the continued operation of its nuclear power plants. By 2018, Westinghouse was supplying nuclear fuel to 7 of Ukraine's 15 nuclear power plants, while Rosatom supplied the rest.[43]

However, disinformation campaigns have continued, including informally. An announcement of fuel supplies for Ukrainian nuclear power plants by Westinghouse led to many critical comments by Russian experts and fake news predictions that a "second Chernobyl" could result.[44] Given the Kremlin's propensity to use information warfare, false reports by Russia suggesting malfunctions in the nuclear plants could cause panic in a population traumatized by the Chernobyl disaster. Lithuanian authorities are also concerned about such a scenario given that Russian firms are building a nuclear power plant in Belarus, just 12 miles from the Lithuanian border and 30 miles from the capital city of Vilnius.[45]

In the aftermath of Chernobyl, authorities in Moscow sought to hide the Chernobyl disaster from the domestic and international public. This resulted in higher human and economic losses, the results of which linger to the present day, undermining public confidence in the region.

Analytical Approach

As demonstrated by the case studies described in the preceding section, energy dependencies constitute a risk multiplier—they create new threats, expand vulnerabilities, expand resilience requirements, and generate cascading and escalating failures. Therefore, it is important to assess the potential consequences of dependency failures and develop approaches to prevent and manage escalating failures. Integrating infrastructure dependency analysis in risk management supports the development of resilience-driven strategies that can be adapted to local and regional needs.[46]

Analysts can use a systemic approach that combines top-down and bottom-up regional analysis to manage these complexities and to establish the appropriate scope of analysis, as well as the specific assets and subsystems for which resilience-related information should be collected.[47]

Figure 2 illustrates an analytical approach to regional dependency analysis.

[41] Fireflyfans (2015) "Oh No! Kiev plans to jam (nuclear) square pegs into round holes," January 12. Available at http://www.fireflyfans.net/mthread.aspx?tid=58977. Accessed October 3, 2018.

[42] Timtchenko, Ilya (2018) "Westinghouse seeks bigger share of nuclear fuel supply," Kyiv Post, June 8. Available at https://www.kyivpost.com/business/westinghouse-seeks-bigger-share-of-nuclear-fuel-supply.html. Accessed October 4, 2018.

[43] Ibid.

[44] Slobodian, Nataliia (2016) "Energy instruments of 'hybrid warfare,'" Stratfor Worldview, March 7. Available at https://worldview.stratfor.com/article/energy-instruments-hybrid-warfare. Accessed September 30, 2018.

[45] Standish, Reid (2017) "Lithuania, Leery of Moscow, Spars with Belarus over Nuclear Reactor," Foreign Policy, October 31. Available at https://foreignpolicy.com/2017/10/31/lithuania-leery-of-moscow-spars-with-belarus-over-nuclear-reactor/. Accessed October 8, 2018.

[46] United Nations Office for Disaster Risk Reduction (2017) Words into Action Guidelines: National Disaster Risk Assessment. C. Cross-Sectoral and Multi-Risk Approach to Cascading Disasters, Available at https://www.preventionweb.net/files/52828_ccrosssectoralmultirisk[1].pdf. Accessed September 28, 2018.

[47] Carlson, L., et al. (2012) Resilience Theory and Applications, ANL/DIS-12-1, Argonne National Laboratory, Decision and Information Sciences Division, Argonne, Ill., USA. Available at https://publications.anl.gov/anlpubs/2012/02/72218.pdf. Accessed September 28, 2018.

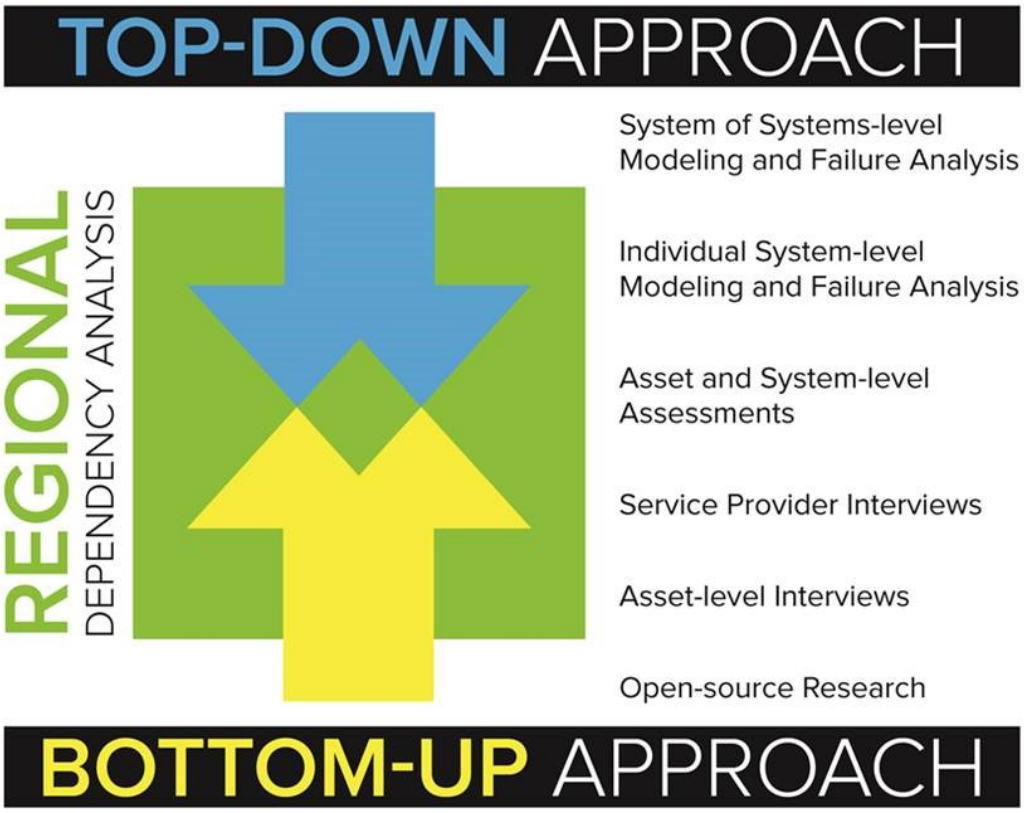


Figure 2: Regional Dependency Analysis[48]

This approach is based on the assumption that a community or region operates as a "system of systems," in which critical infrastructure assets and systems can be analyzed as part of a broader system of infrastructure. In this systemic approach, top-down analyses characterize high-level system operations and help identify cascading and escalating failures within individual systems. Ultimately, top-down analyses help identify supply areas that would potentially be affected by the loss or degradation of the resource supplied by the critical infrastructure considered (e.g., areas without electric power).

Bottom-up analyses characterize asset-level operations and help identify first-order upstream and downstream dependencies. Ultimately, bottom-up analyses characterize how asset-level operations would react to the loss or degradation of a resource. Considering energy systems, top-down analyses can allow analysts to identify areas where, for example, natural gas supply shortages could occur. Bottom-up analyses conducted in these areas allow analysts to determine how specific critical assets would react to a natural gas shortage. For example, natural gas-fired electric power-generating plants cannot operate without a supply of natural gas. Including the degradation of the generating plant in electric power top-down analyses allows analysts to identify areas that could experience blackouts.

Considering energy infrastructure's operating environments (e.g., policy, regulation, geopolitics) with the four dependency classes produces an optimal analysis for comprehensively understanding energy dependency and interdependency dimensions. Through these activities, decision makers can anticipate and characterize how energy dependency and interdependency dimensions influence the protection and resilience of critical infrastructure systems targeted by hybrid operations. This effort requires a collaborative environment that promotes information sharing and multidisciplinary analyses. The overall analysis must expand beyond consideration of critical infrastructure to consider geopolitical, political, and economic characteris-

[48] Petit, Frederic, Duane Verner, and L.A. Levy (2017) Regional Resiliency Assessment Program Dependency Analysis Framework, ANL/GSS-17/05, Argonne National Laboratory, Global Security Sciences Division, Argonne, Ill. USA.

tics.

Table 1 – Optimal Energy Dependency Analysis to Combat Hybrid Threats

Table 1 presents a general overview of the data, analysis, and output characterizing an optimal analysis.

Data Collection	*Analysis*	*Output*
Includes both geopolitical dependency categories and critical infrastructure dependency classes. Collected through a variety of mechanisms, including surveys, academic research, and open source information.	Integrates infrastructure modeling and failure analysis, including cascading and escalating failures. Considers the fungiblity of energy resources, market conditions, and other dynamic factors.	Enhanced situational awareness of hybrid threats to energy systems. Integrated understanding of potential cascading and escalating failures from the local to the global level. Insight into hybrid-threat actors' capabilities and intentions.

Recommendations

Current energy security considerations include a number of factors, such as different geopolitical dependencies and classes of dependencies in infrastructure. Cybersecurity, information warfare, and geopolitical tensions require continued risk assessment and resilience contingency planning. The increasingly interconnected global energy markets, including the gas and nuclear sectors, can implicate EU and NATO member states in the energy security risks of members of their alliances and beyond.

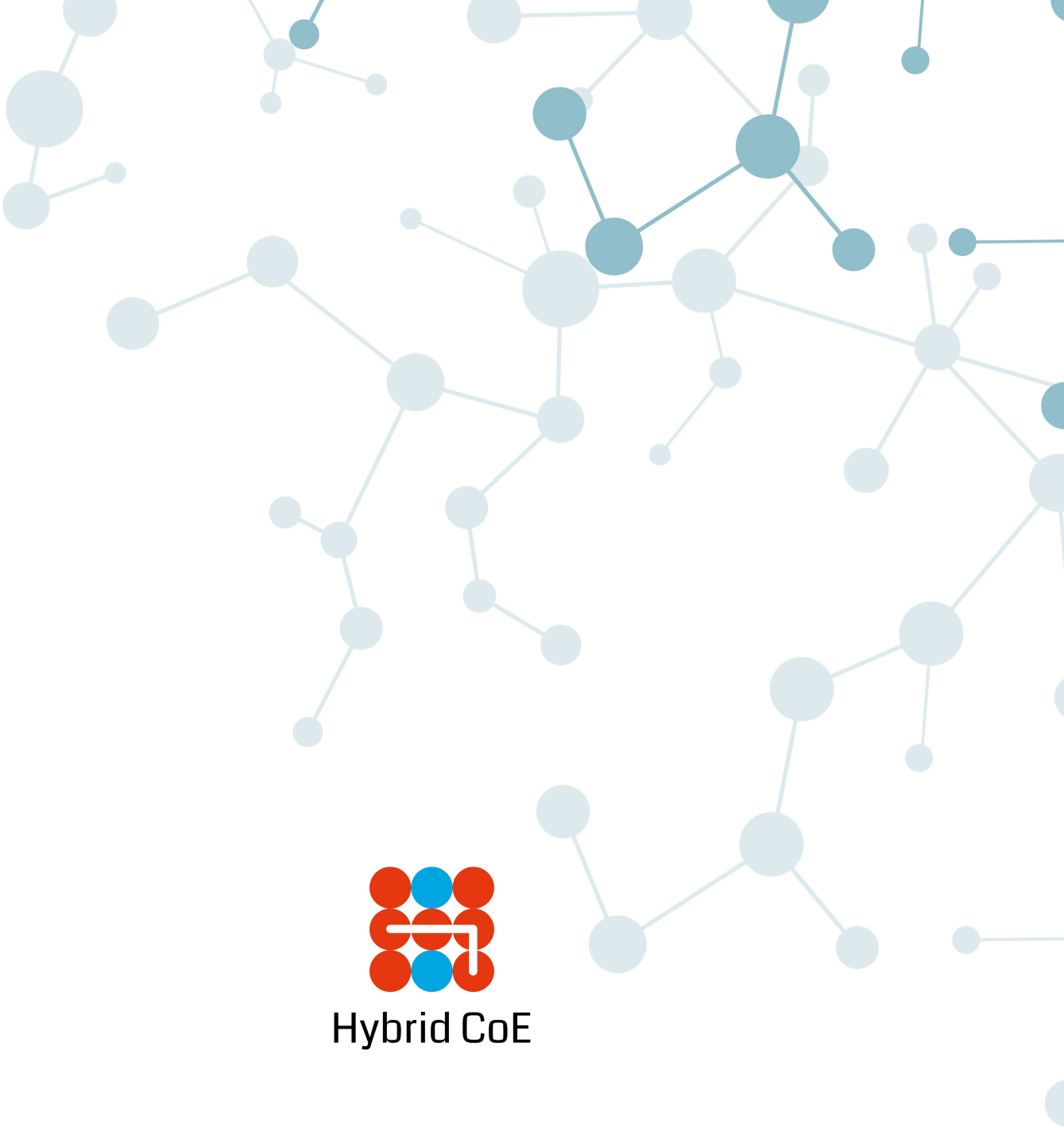
Because of the interconnected nature of energy infrastructure, Hybrid CoE member nations and allied organizations should consider adopting a common approach to assessing risk associated with energy dependencies in the age of hybrid threats. The U.S Department of Homeland Security's (DHS) Regional Resiliency Assessment Program (RRAP) provides a best-practice assessment of critical infrastructure dependencies. Initiated by the DHS Office of Infrastructure Protection in 2009, the RRAP addresses a range of infrastructure resilience issues that could have significant regional, national, and cross-border consequences.[49] Recently adopted by Public Safety Canada, and implemented through cross-border projects with the United States, the RRAP provides a process that can be replicated to help organizations measure and improve their resilience to all hazards, such as cyber threats, accidental or intentional manmade events, and natural catastrophes.[50] The RRAP is an ideal framework in which to incorporate energy infrastructure's operating environment (e.g., policy, regulation, geopolitics) with the four dependency classes (i.e., physical, cyber, geographic, and logical) to produce an optimal analysis for comprehensively understanding energy dependency and interdependency dimensions and associated risks in the age of hybrid threats.

In addition, Hybrid CoE member nations and allied organizations should share best practices and expertise on combating hybrid threats to energy systems through the Hybrid CoE's Energy Network. As part of the Hybrid CoE's Vulnerabilities and Resilience Community of Interest (COI), the Energy Network facilitates multinational and multidisciplinary collaboration so that member nations and institutions can better understand, defend against, and respond to hybrid threats. Specific outcomes from the Energy Network COI will include the following:

- Improved understanding of hybrid threats and vulnerabilities to energy supply networks,
- Increased resilience through shared best practices and new policy proposals,
- Improved application of existing policies and funding programs,
- Improved public-private partnerships in countering hybrid threats and improving resilience,
- Promotion of potential business solutions and regulatory frameworks at national and community levels, and
- Proposed topics for academic research.

[49] DHS (2017) "Regional Resiliency Assessment Program," last published September 22. Available at https://www.dhs.gov/regional-resiliency-assessment-program.
Accessed October 3, 2018.

[50] Public Safety Canada (2018) "The Regional Resilience Assessment Program," modified August 13. Available at https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-rrap-en.aspx.
Accessed October 3, 2018.



Hybrid CoE

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

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.

ISBN 978-952-7282-15-1