Assessing Threats to South Korea’s Undersea Communications Cable Infrastructure

Sean O’Malley

Undersea communications cables are critical infrastructure for the national security of South Korea. As an isolated, peninsular state, South Korea depends on these cables as its lifeline to the international community. Nonetheless, compared to its alliance partner the United States, South Korea designates fewer of its own cable systems as critical and has no uniform approach for assessing threats and protecting this indispensable infrastructure. Using a design basis threat (DBT) framework, this paper assesses the threat environment of Northeast Asia for South Korea’s undersea communications cable infrastructure, and clarifies the role of the South Korean state in protecting this infrastructure. In order to achieve these two goals, this analysis provides a threat assessment based upon South Korea’s traditional geopolitical conditions and the submarine and cyber capabilities of regional state actors—North Korea, China, Russia, and Japan. Conclusions suggest that South Korea’s undersea cables are at risk from numerous geopolitical threats and the state should participate more actively in protecting these vital lines of communication.

Key Words: Cyber, Infrastructure, Northeast Asia, South Korea, Undersea cables

There are more than four hundred undersea communications cables in the world providing ninety-nine percent of all international digital communications traffic: military communications, economic communications, and social communications. Yet despite this ubiquity, security analysts in the social sciences have devoted scant attention to this critical infrastructure (CI).

* Sean O’Malley is an associate professor in the Department of International Studies, Dongseo University, Busan, South Korea. He holds an MS in Political Science from Portland State University and a PhD in International and Area Studies from Pukyong National University. Prior to graduate studies, he was a network operations center technician on the Oregon end of the Southern Cross undersea cable. His research interests include cybersecurity, regionalism, and middle power relations. Email: seanmo@dongseo.ac.kr
For the Republic of Korea (hereafter South Korea), the lack of attention could be devastating. South Korea is almost wholly dependent on its undersea communications cable infrastructure (UCCI) for international communications, so much so that it is difficult to overstate the importance of UCCI for maintaining global connectivity and societal well-being of the country. For a state with no alternative, terrestrial, interstate connections for telecommunications traffic, these cables are South Korea’s lifeline to the international community. South Korea’s UCCI should be one of the greatest national security concerns for the state, but it receives virtually no attention in the social science literature on Korea. If these cables are targeted for aggression and disrupted or destroyed, the South Korean economy will come to an immediate standstill and military operations may be crippled. The importance of these cables is underscored by their designation as CI by the state.

This paper is a rarity, as it focuses solely on South Korea’s undersea communications cables from a national security perspective. South Korea resides in the tension-filled region of Northeast Asia, where it is surrounded by potentially hostile neighbors who are increasingly competitive in security and economic affairs. Therefore, using a modified form of the design basis threat (DBT) framework developed by the International Atomic Energy Agency for CI, this paper attempts to 1) assess the threat environment of Northeast Asia for South Korea’s UCCI, and 2) clarify the role of the South Korean state in protecting its UCCI. In order to achieve these two goals, this analysis provides a threat assessment based upon South Korea’s traditional geopolitical conditions and the submarine and cyber capabilities of regional state actors—the Democratic People’s Republic of Korea (hereafter North Korea), the People’s Republic of China (hereafter China), the Russian Federation (hereafter Russia), and Japan. In an era when discussions abound of the coming technology wars between developed states, protecting the fundamental systems underlying the networked world never seemed more important. For South Korea, it is imperative.

It is hoped the security analysis presented here helps deepen understandings of undersea communications cables as CI, especially for social scientists, while illuminating the threats they face. Following this introduction, part two of the paper provides a basic explanation of UCCI as physical and critical infrastructure. Part three explains design basis threat as a method and framework and provides a threat-actor typology. Part four is a threat environment analysis of Northeast Asia with a focus on the geopolitical conditions and the capabilities of Northeast Asian threat actors, and the paper concludes with recommendations for
policymakers. Although it may seem odd to some Northeast Asia watchers that Japan is considered here as a threat actor to South Korea’s security, it should be noted that the South Korea-Japan rivalry dyad is the fifth most active cyber conflict dyad according to Valeriano and Maness (2014, 356). This fact and recurrent tensions between the two states seem reason enough to include Japan in the following analysis.

UNDERSEA COMMUNICATIONS CABLE INFRASTRUCTURE

UNDERSTANDING UCCI AS PHYSICAL INFRASTRUCTURE

The basic components necessary for undersea communications cables are not terribly complex from a physical perspective. In the simplest terms, these components include the cable, branch units, cable landing stations, and a network operations center. A cable system can be likened to a subway line with its tunnels, switches, stations, and transportation control center. Submarine cable landing stations sit on or near the shoreline, on opposite sides of a large body of water. Two stations, often in different countries, terminate the length of the main submarine cable. Off the main cable, shorter cable segments can be run to a third country’s shore from a branch unit, thereby allowing one cable system to connect multiple states. The Asia Pacific Gateway cable, for example, connects eight different countries in East Asia. Overall, it has nine branch units allowing the cable to terminate at eleven different cable landing stations—two stations for the main cable and nine stations for shorter segments. Inside a cable are optical fibers through which data travels from one station to the other. If needed, data signals can be routed to shorter cable segments via the branch unit. The cable and the data moving through it are monitored from the network operations center, where network management systems and other equipment allow the cable’s operator to monitor the system for status, faults, and errors, as well as adjust the configuration of system equipment when necessary (for more detail see Chesnoy 2016, 9). Like most infrastructure systems today, fiber optic cable systems depend on networked communication for their management and monitoring. This makes them susceptible to hacking and other types of cyber aggression in addition to more traditional, physical aggressions against CI.

Currently, South Korea has nine undersea communications cables in operation and one cable in the survey phase of the project. Nevertheless, as the EAC-C2C cable has segments landing at Taean and Busan, South Korea has eleven cable landings ashore. To accommodate these eleven landings, there are four cable landing stations—two on the southeast coast in Busan, one on the southern
island of Keoje, and one on the west coast in Taean (see table 1). Importantly, every cable landing in South Korea also lands in either Japan or Taiwan, and all cables but one—the Korea-Japan Cable Network—land in China.

Table 1. South Korea’s Current Undersea Cable Infrastructure

| CLS          | CLS operator     | Cable name                  | Cable owner                                      |
|--------------|------------------|-----------------------------|--------------------------------------------------|
| Busan CLS    | KT Submarine     | APCN-2                      | Consortium                                       |
|              |                  | Asia Pacific Gateway (APG)  | Consortium (includes KT Corp. and LG Uplus)       |
|              |                  | FLAG North Asia Loop (FNAL) | FNAL—Global Cloud Exchange                       |
|              |                  | /REACH North Asia Loop (RNAL)| RNL—FLAG Telecom, Level 3 Communications         |
|              |                  | Korea-Japan Cable Network   | KEPCO, Softbank Telecom                          |
|              |                  | (KJCN)                      |                                                  |
|              |                  | New Cross Pacific (NCP)     | Consortium (includes KT Corp.)                    |
|              |                  | Cable System                |                                                  |
|              |                  | Southeast Asia-Japan Cable  | Consortium (includes SK Telecom)                  |
|              |                  | 2 (SJC2) (planned 2020)     |                                                  |
| C2C Busan    | Sejong Telecom   | C2C (of EAC-C2C)            | Telstra                                         |
| CLS          |                  |                             |                                                  |
| Keoje CLS    | KT Submarine     | Flag Europe-Asia (FEA)      | Cloud Exchange                                   |
|              |                  | SeaMeWe-3                   | Cyprus Telecommunications Authority, TM Berhard,  |
|              |                  |                             | TATA Communications, Sea-Me-We 3 Consortium      |
|              |                  | Trans-Pacific Express (TPE) | China Telecom, China Unicom, Chungwha Telecom,   |
|              |                  | Cable System                | Verizon                                          |
| Taean CLS at | Dacom Crossing   | EAC (of EAC-C2C)            | Telstra                                         |
| Shindu-ri    |                  |                             |                                                  |
|              |                  |                             |                                                  |

Note: Adapted from O’Malley (2019, 318). CLS = cable landing station; CLS operator retrieved from Submarinenetworks.com; Cable name per CLS retrieved from TeleGeography; Cable owner information in STF Analytics (2018).

Unlike ports, power plants, civil aviation systems, and other CI under state protection, submarine communications cables traverse multiple jurisdictions and therefore lack a single sovereign identity. Most management and operations issues, including security and protection, are within the purview of the private companies that own the cables. With corresponding international legal and governance structures, Davenport (2015, 66) concludes that “submarine cables are the very essence of transnational infrastructure.” They seem to be the embodiment of global cooperation and market mechanisms in the most positive
sense. Nonetheless, beyond the global governance and cooperation in regards to UCCI, interstate relations and national security have a significant role to play.

THE IMPORTANCE OF UCCI AS CRITICAL INFRASTRUCTURE
Globally there are more than four hundred undersea communications cables in use domestically, internationally, or in the planning stages connecting all continents except Antarctica (STF Analytics, 2018). Furthermore, UCCI are “operational with up to ‘5 nines’ reliability, or 99.999 percent of the time,” (Sechrist 2012, 9) which means there is little opportunity for a failure to put them in the spotlight. However, when the Hengchun earthquake severed nine of eleven cables off the coast of Taiwan in 2006, the “fallout included loss of internet connectivity for most of Hong Kong; a sixty percent loss of international calling capacity from Taiwan to the United States; and Korea’s financial markets mostly halted trading of the Korean won due to communication problems” (O’Malley 2019, 316 paraphrasing Sechrist et al. 2012). Therefore, from a national security perspective, the transnational nature of the submarine cable physical infrastructure and the far-reaching effects of any communications disruptions must be a concern.

In the first US National Infrastructure Protection Plan (NIPP) (2009, 128-129) undersea cables and associated facilities fell under the sections on linkages of dependencies, interdependencies, and global aspects of US critical infrastructure and key resources (CIKR). It was understood that these assets would require the efforts of foreign countries and foreign private entities to help manage associated risks (ibid.). Around the same time that NIPP 2009 was being finalized, and seemingly in accordance with its recommendations, the US Department of State listed seventy-one undersea cable landings overseas as CIKR out of three hundred CIKR listed. Undersea cable landings therefore accounted for nearly twenty-four percent of all US overseas CIKR. That list of seventy-one cable landings included four landings in South Korea at three different stations—both segments of the EAC-C2C cable, the FLAG/REACH North Asia Loop, and the KJCN (WikiLeaks 2010). Only South Korea’s Keoje cable landing station did not have a landing considered as US overseas CIKR.

Interestingly, in October 2015, South Korea’s Ministry of Science, ICT and Future Planning designated only one cable landing station as CI—the Busan CLS under KT Submarine which houses six cables (Ministry of Science, ICT and Future Planning 2015). At the time, the now retired China-US Cable Network was listed among the six, as opposed to the more recent SJC2 cable system, which is still in the survey phase. It seems odd that South Korea and the United States, as military alliance partners, do not have the same landing stations listed
as CI. After all, they are heavily reliant on UCCI for military communications, as implied by the US CIKR designations. A more recent concern is that South Korea’s newly acquired F-35 combat aircraft “cannot operate effectively unless it is in constant contact with the Autonomic Logistical Information System (ALIS) that Lockheed maintains at its Fort Worth facility. If this link was cut, any F-35s operated outside of the continental United States would cease to function at full capability (Defense-Aerospace.com).” Currently, these data transmissions depend in part on the reliability of UCCI.

In addition, figures indicate South Korea is a hyper-connected society and export-driven economy heavily reliant on international financial transactions. South Korea is ranked first in Asia and the Pacific and second globally in the International Telecommunication Union’s Information Communication Technology Development Index (2017, 65). Some 95.1 percent of individuals in South Korea have an internet connection, with fixed-broadband subscriptions at 41.6 per one hundred people and mobile-broadband subscriptions at 112.8 per one hundred people (Broadband Commission for Sustainable Development 2018, 80-86). The country’s international bandwidth usage equated to approximately 4Tbps (terabits per second data throughput) in 2016 and saw a forty-two percent average growth rate from 2012-16 (Xiong 2017, 9). In addition, according to the World Bank, exports of goods and services (Databank 2019a) account for 43.1 percent of South Korea’s 1.53 trillion dollar economy (Databank 2019b). Although exact financial data is difficult to ascertain, global undersea cables transmit in excess of ten trillion dollars per day in financial transactions (Nagpal 2018, 28; Sechrist 2012, 9) and foreign entities had claims of nearly 408 billion dollars on counterparties in South Korea at the end of September 2018 (Bank for International Settlements 2019). Broadband subscriptions, high export volumes, and foreign bank claims taken together indicate the country probably does tens of billions of dollars per day in financial transactions via UCCI, in addition to data and voice traffic that is not financial in nature. This means that South Korea’s social and economic fabric is vulnerable to disruption if the state’s cables are compromised.

THE DESIGN BASIS THREAT METHOD

In order to minimize disruptions in the operations of CI, it is important to assess potential threats to security. One tool for such an assessment is a design basis threat. According to the International Atomic Energy Agency (2009, 1), “A design basis threat (DBT) is a comprehensive description of the motivation,
intentions and capabilities of potential adversaries against which protection systems are designed and evaluated.” The purpose of a DBT is to uncover the characteristics and attributes of adversaries that may wish to commit a malicious act against a physical facility target, though the DBT “is not intended to be a statement about actual, prevailing threats” (ibid.). In this regard, the DBT does not name specific adversaries and it is not meant to be a procedural guide to manage specific scenarios or adversarial tactics. Rather, the DBT is meant to provide a baseline of threat capabilities at which the state takes primary responsibility for protection of a facility from a private operator. It is also meant to provide a maximum level of threat capability against which protection is reasonably ensured (see figure 1).

A DBT analysis in its strictest sense is highly improbable in an academic setting, as the analysis requires access to government intelligence, some of which may be classified, and government decision-making to determine resource allocation and roles or areas of responsibility. Still, the DBT method applied by non-governmental entities can be useful in that it allows a researcher to determine threat statements, highlight adversarial capabilities, and suggest
physical facility protections that may otherwise be underappreciated. It is used here for these purposes.

DEFINING A THREAT TO CRITICAL INFRASTRUCTURE
The first step in a DBT is the threat analysis. This analysis “shows the range of all threats, from a condition of low threat capabilities (at the bottom of the chart), to high threat capabilities (at the top of the chart). This range represents the known, actual and prevailing threats that are evaluated in the threat assessment (ibid., 5)” (see figure 1). The US Department of Homeland Security’s DHS Risk Lexicon defines threat as a “natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property” (Risk Steering Committee 2010, 36). DHS later refined the concept in The Strategic National Risk Assessment in Support of PPD-8, when it categorized national level events in three threat categories: natural, technological/accidental, and adversarial/human-caused (DHS Office of Risk Management and Analysis 2011, 2-4). Furthermore, the recent US factsheet on Joint National Priorities for Critical Infrastructure Security and Resilience specifically calls for “particular focus on safeguarding critical infrastructure from potential cyber threats driven by hostile nation-states (Department of Homeland Security 2018, 2).”

In the case of South Korea, CI and cybersecurity seem deeply intertwined and all too often it appears the government is reactive instead of proactive. The denial of service cyber attacks of March 4 and April 12, 2011 spurred the development of the National Cyber Security Master Plan, which did call for securing a dedicated workforce for the protection of core national infrastructure—one of many recommendations (Korea Internet Security Agency 2015, 12-14). The cyber terror attacks of March 20 and June 25, 2013, were the impetus for the National Cyber Security Comprehensive Countermeasures put forth by the Ministry of Science, ICT and Future Planning (2013, 1). That document assigned the Blue House (the office of South Korea’s sitting president, akin to the US White House) as a cybersecurity control tower; the National Intelligence Service was tasked with establishing a cybersecurity working group; and relevant central administrative agencies, like the Ministry of Science, ICT and Future Planning and the Ministry of Defense, were responsible for establishing cyber response systems for their respective fields (ibid.). The 2014 cyber terror attacks on nuclear power plants operated by Korea Hydro and Nuclear Power, resulted in the heightened awareness on the part of society and the government to cyber attacks on CI (Lee and Lim 2016, 869). Most recently, in April 2019, the National Security Office of the Blue House released Korea’s first National
Cybersecurity Strategy. A rather short document offering few specifics and only general direction, the paper’s technical shortcomings are somewhat made up for by the symbolism that cybersecurity has finally reached the foreground of defense strategy thinking at the highest levels of the government.

Despite the presence of a control tower and input by the presidential office, there has been consistent grumbling among the private research sector that the government lacks a unified, comprehensive approach to cybersecurity, as it has distributed responsibility for countermeasures across ministries (see Bak and Lee 2017; Hong 2019; Lee and Lim 2016). Although inefficiencies in a response system are troubling, the lack of a consistent definition for threat is more worrisome. The Act on the Protection of Information and Communications Infrastructure (Act No. 15376) of 2018 has no definition for threat, but Article 2 does have definitions for electronic intrusion and intrusion incident. The 2018 Act on Measures for the Protection of Nuclear Facilities, etc. and Prevention of Radiation Disasters (Act No. 15280) does define threat in the context of CI, but it is limited to

(a) Sabotage; (b) Electronic infringement; (c) Using nuclear materials to harm human life and bodies or inflict damage on property or the environment; (d) Acquiring nuclear materials to compel individuals, corporations, public institutions, international organizations, or nations to commit a specific act.

Article 7 of the 2017 Presidential Decree 28211, pursuant to Act No. 15280, requires a design basis threat analysis for nuclear facilities every three years to determine threat factors, the possibility of threat occurrence, and the results of threat occurrence. However, no such prescription is found in the Act on the Protection of Information and Communications Infrastructure (Act No. 15376) or in Presidential Decree 29421 pursuant to that act. Rather that act and the subsequent decree require the analysis and evaluation of vulnerability to this critical infrastructure—the method of analysis to be determined by the head of the relevant central administrative agency.

Comparatively speaking, the Korean and US systems of critical infrastructure protection are therefore fundamentally different. The US system requires multiple federal agencies to follow the DHS Risk Lexicon definition of threat and provide DBT analyses reflective thereof, providing some consistency across agencies in threat analysis. The Korean system makes the definition of threat incumbent on each administrative agency for their respective CI. In addition, central administrative agencies may perform DBT or vulnerability analyses pursuant to the relevant laws, making consistent analysis across agencies very
difficult if not impossible. The lack of consistency may seriously hinder effective security and responses to aggressions.

THREAT ANALYSIS FOR UCCI

There are two general categories of threats that may affect UCCI: physical and cyber. The threat actor typology developed by Khalizad (1999, 407) for information-warfare takes account of both, as does the modified threat actor typology for cyberspace put forth by RAND Europe (Robinson et al. 2012, 6). Table 2 shows one more evolution of this typology for use with UCCI, though one must remember that a DBT assessment must account for more than just man-made threats and actors, if following the DHS’ definition of threat. In its analysis of UCCI, the United States Office of the Director of National Intelligence (2017, 9-10) categorized threats as natural, accidental, and malicious, in accordance with DHS guidelines. None of the threats under the categories of natural or accidental would warrant a threat statement—they would be operator responsibility. The malicious category however includes cyber attack, vandalism, activism, theft, terrorists, and state-actors. Of these, threat statements could easily apply to cyber attack, terrorists, and state-actors.

Table 2. Threat Actor Typology for UCCI

| Type                          | Subtype                     | Goal                                  | Probable Method |
|-------------------------------|-----------------------------|---------------------------------------|-----------------|
| Individuals                   | Grey hat, Black hat         | Mayhem, joyride, minor vandalism      | Cyber           |
| Coordinated sub- or pannational groups or networks | Criminal groups             | Money, power                          | Cyber           |
|                               | Commercial organization     | Industrial espionage, sale of information | Cyber           |
|                               | Hacktivist (anarchic/millennial) | Protest, fear, pain, disruption | Cyber           |
|                               | Insurgent groups            | Overthrow of a government or separation of a province | Cyber or kinetic means |
|                               | Terrorists                  | Gaining support for and deterring opposition to a cause; sow fear, pain, disruption | Cyber or kinetic means |
| State                         | Rogue†                      | Deterring, defeating, or raising the cost of a state's involvement in regional dispute | Cyber or kinetic means |
|                               | Peer-competitor‡            | Deterring or defeating a country in a major confrontation, espionage, economic advantage | Cyber or kinetic means |

Note: Adapted from Khalizad 1999 and Robinson et al. 2013.
† A rogue state is considered here to be a state that may act irrationally and commit an unprovoked hostile act at any time.
‡ The term peer competitor can be a bit murky. Here it is used to refer to a state that has both the capabilities and intentions to pursue hostile acts against the state being analyzed, if a local or regional crisis erupts. In this sense, the term utilizes the two components (capabilities and intentions) that RAND considers essential (see Szayna et al., 2001, 7–43).
When it comes to state-actors, the threat actor typology tells us that rogue states and peer-competitors may have various goals for aggression, anything from defeating a country in confrontation to economic advantage. They may use cyber or kinetic means to achieve these goals. Such means may be carried out by insider or outsider actions. For the analysis of outsider threat actions by regional state-actors, there are three facets of UCCI’s physical facilities that require consideration: the undersea cable, cable landing stations, and networked facility equipment. Undersea cables are submerged and aggression will therefore occur underwater; cable landing stations and network operations centers are above ground facilities that are susceptible to armed assault and aerial strikes; and networked facility equipment is a prime target for cyber attack. The following are reasonable, though general, threat statements regarding these facets:

1) Cutting or tapping of undersea communications cables via submarine, submersible vehicle, surface ship, or human diver. The cutting of cables can be performed on a single cable or multiple cables in a chokepoint with cables damaged by dissection in one or more locations or damaged by explosives along a length of cable. The tapping of a cable through technological means to siphon data can occur along any length of the cable.

2) Cable landing station sabotage or destruction by a violent and determined adversary via aerial attack or armed assault using land-based or water-based transportation.

3) Cyber attack on plant facilities including power feeding equipment, submarine line terminating equipment, and network equipment.

Of these three threat statements, the first and last will be assessed below. As cable systems are privately owned, the security of the cable landing station against low level threats and physical assault would be the responsibility of the system operator, while high level threats like an aerial attack would go beyond the DBT analysis and fall under the purview of inherent protection that is reasonably ensured, e.g., military operated anti-missile or anti-aircraft defenses. Sechrist (2012, 15) believes that “Poor physical security of cable landing sites is a potential Achilles heel for US and global cyber security,” and that “Cable landing sites have always been and continue to be single points of potentially catastrophic attack and failure that must be addressed.” Physical security of a cable landing station would often entail a fenced building with CCTV cameras and locked doors with electronic security measures to approve entry. These often innocuous looking buildings seem to rely on the disinterest of people to thwart low-level vandals and criminal elements (for a typical description, see Blum
However, a determined adversary would be able to identify and breach many of these buildings. South Korea’s Dacom Crossing has even put the layout of their Taean cable landing station online, which is a poor approach at security for a station listed as CIKR by the United States (see Dacom Crossing). Although not covered extensively here due to their private nature, physical security of cable landing stations should be heavily coordinated by the state and operating entity. Some recommendations to enhance cable landing station security are shared in this paper’s conclusions.

THE THREAT ENVIRONMENT OF NORTHEAST ASIA

TRADITIONAL GEOPOLITICAL CONDITIONS
Before discussing the threats of cable cutting, cable tapping, and cyber attacks in regard to South Korea’s UCCI, one should look at the threat environment of Northeast Asia. South Korea sits in a rather precarious position. Firstly, it has no terrestrial telecommunications infrastructure to the greater Asian continent. It is solely dependent on its maritime environment to accommodate the communications and transport infrastructure it requires to participate in the international community. This is due to the fact that at the end of World War II, the United States and Soviet Union divided the Korean peninsula, a former colony of Japan, at the 38th parallel. Construction of a heavily fortified demilitarized zone reinforced this division after the devastating Korean War (1950-53) ended in an armistice, leaving North Korea and South Korea technically at war. Secondly, all but two of South Korea’s undersea communications cables traverse the Western Channel of the Korea Strait between Korea’s southern coast and the Japanese island of Tsushima. This means most cables pass through an area of the sea that is only fifty kilometers wide and averages approximately ninety meters of depth where these cables converge (Korea Hydrographic and Oceanographic Agency 2011). This is an incredibly narrow and shallow chokepoint—a network point of concentration where many cables come together (O’Malley 2019, 320). These two unique vulnerabilities would seem to make South Korean UCCI an intriguing target in times of hostility, and the JoongAng Ilbo (2019) claims tensions are rising.

South Korea’s closest northern neighbors are North Korea, China, and Russia. These three are authoritarian states of varying types with either friendly or convenient relations among each other, including a mutual friendship treaty between China and North Korea and an agreement on preventing dangerous military action between Russia and North Korea. Within a span of four days,
July 22-25, 2019, North Korea released images of what appeared to be a new ballistic missile submarine (Trevithick 2019) and launched two short-range ballistic missiles into the East Sea (Oh 2019); the JoongAng Ilbo newspaper reported that South Korea’s National Intelligence Service had arrested a suspected North Korean spy sent by the North’s elite Reconnaissance General Bureau—the thirty-fifth spy to be apprehended since 2008 (Kim 2019); China released its 2019 defense white paper within which it claimed South Korea’s Terminal High Altitude Area Defense (THAAD) anti-missile system “deployment ‘gravely damaged’ the strategic balance and security interest in the Asia-Pacific region” (Choi 2019); Chinese and Russian military aircraft during joint exercises violated South Korea’s air defense identification zone—the thirty-eighth violation by those states this year (Jo 2019); and one Russian early warning aircraft penetrated South Korea’s sovereign airspace, prompting South Korean warplanes to fire hundreds of warning shots (JoongAng Ilbo 2019; Osborn and Lee 2019).

South Korea’s southern neighbor, Japan, has also been in the news. A traditional friend of South Korea and an alliance partner of the United States, Japan and South Korea have an intelligence sharing agreement—the General Security of Military Information Agreement—to coordinate better threat response. Still, in March 2019, South Korea’s Yonhap News ran an article on potential threats to Korea accompanied by an image of the Japanese flag. The article stated that “Japan posed threats to South Korean warships with menacing low-altitude flybys” (Song 2019). Then, amid an escalating crisis and claiming the collapse of mutual trust between the states, Japan slapped export controls on three chemicals necessary for South Korea’s semiconductor and plasma display manufacturing industries (Yonhap News 2019a). This was followed by Director Chung Eui-yong, of South Korea’s presidential National Security Office, claiming that continuance of the General Security of Military Information Agreement “can be reconsidered in accordance with (relevant) situations” (Yonhap News 2019b). Some time later, the Blue House announced it would discontinue the Agreement in November 2019. A rift in security and economic relations, along with historical grievances and territorial disputes, deepens mistrust between these two states, even though they are both democracies and close friends of the United States. Taken together, the menacing flybys, airspace incursions, sabre-rattling, and spies indicate that South Korea faces a number of kinetic challenges from its neighbors.
CABLE CUTTING AND CABLE TAPPING CAPABILITIES OF REGIONAL THREAT ACTORS

Included in kinetic challenges may be cable cutting and cable tapping. Submarine communications cables are not really designed with properties protecting them from intentional aggression. Submarine cables have been cut by anchors and stolen by pirates. Cable cutting is not that difficult to do, could have serious effects, and has a long history. The United States cut undersea cables during the Spanish-American War in 1898 (Winkler 2015) and the Russians used fishing trawlers to cut cables during the Cold War (Coates 2015). More recently, two fishing boats stole eighty metric tons of cable off the seafloor in Vietnam, one incident of many that added up to five hundred metric tons of stolen cable in a six month period (LIRNEasia 2007). As noted, most cables landing in South Korea pass through a chokepoint between the southern coast of the peninsula and Japan’s Tsushima Island. With an average depth of ninety meters, these cables are susceptible to aggressions from human divers, surface ships, and submersible vehicles. After a North Korean fishing vessel sailed undetected for two and a half days and arrived on South Korea’s shores 130km south of the maritime Northern Limit Line in June 2019 (Jung 2019), one must wonder what kind of asymmetric threat North Korean fisherman pose and ponder the damage they could cause, let alone the threat from more sophisticated surface vessels of other regional actors. Suffice it to say that every regional state actor has the means by which to cut cables.

Compared to cable cutting, cable tapping is a much more specialized skill. The states of Northeast Asia are involved in a rising competition of technonationalism, so much so that in 2019 Global Asia dedicated its March 19 issue to the phenomenon of “Technology Rivalry and the Rise of Nationalism.” There is acknowledgment that any potential for victory in the coming technology wars will depend on big data—the velocity, volume, and variety of data being created in the wake of man’s ever-increasing digital footprint (see Hilbert 2015). It is UCCI that effectively monopolizes the international transmission of this data.

The importance of this infrastructure to data collection, under national security auspices, was highlighted in large part thanks to former US intelligence analyst Edward Snowden, who notified the world that the US National Security Agency and the United Kingdom’s Government Communications Headquarters were tapping some two hundred undersea cables and siphoning the communications data for analysis (MacAskill, Borger, Hopkins, Davies, and Ball 2013). Though concerns had been raised prior to Snowden’s revelations, they did not capture the popular imagination (Associated Press 2005; Marks 2013). The
Snowden revelation managed to accomplish in popular literature what others had not—it connected state security behaviour and cyber intrusions directly to the underappreciated UCCI. This has led to a deepening of the state security literature in regards to UCCI (for example Carter et al. 2009; Clark 2016; Sunak 2017) and perhaps a modest increase in press coverage of state behaviour under the seas (see Chalfant and Beavers 2018; Matsakis 2018; Tsuruoka 2018).

Today, tapping a fiber-optic undersea cable “requires small specialist submarines secretly diving to great depths. Tamper with a cable down there, and it’s so much harder to locate or repair (Seidel 2019).” Of course tapping makes the tapper privy to military communications as well as all other communications data on the cable. As stated above, both the United States and United Kingdom tap cables. The USS Halibut was tapping cables in the 1970s to “listen in on message traffic to Soviet nuclear forces” (Mizokami 2017); it is believed the USS Jimmy Carter does the job of tapping now (ibid.). Russia is the only traditional friend of North Korea and peer competitor of the United States known to have the capability to tap undersea fiber-optic cables (see Chalfant and Beavers 2018; Matsakis 2018; Tsuruoka 2018). Currently, the Russian submarine Losharik is believed to have tapping technology aboard (Seidel 2019), and NATO is worried that Russia is conducting tapping operations in the North Atlantic (Birnbaum 2017). Though, according to Reichmann (2018), the real worry for NATO revolves around “Russia’s Main Directorate of Deep Sea Research, whose specialized surface ships, submarines, underwater drones and mini subs conduct reconnaissance, underwater salvage and other work.”

Beyond the capability to tap cables, Russia’s motivations to tap may run high. The worry for South Korea should be burgeoning military ties between North Korea and Russia along with deteriorating relations between the United States and Russia. Russia has become the country most visited by North Korean senior officials (Lukin 2016) and the two countries inked an agreement on preventing dangerous military action in 2015 (Byrne 2015). NK News director of intelligence John Grisafi was quoted as stating, “The agreement seems to be about military-to-military and diplomatic communication regarding military and security force operations which could potentially impact the other party (ibid.),” and Lukin (2016) argues that since the Ukraine crisis began in 2013, Russia’s strategic competition with the United States has turned to bitter enmity. If this is true, South Korea and its UCCI may be in Russia’s crosshairs to disrupt military communications among the US military and its alliance partner in times of hostility. Even though Russia has offered to share civilian nuclear technology with its friend (Hudson and Nakashima 2019), it is not known whether Russia is sharing its cable tapping technology with the North Korean General Staff.
Nevertheless, Russia certainly has the technology to seriously disrupt the cable communications of South Korea.

China’s aggressive expansion of naval capabilities, including submarine technology, is also a worry. “The PLAN [People’s Liberation Army Navy] places a high priority on the modernization of its submarine force” and may have a more clandestine land attack option from its submarines in the next decade (Office of the Secretary of Defense 2017, 24). This implies the future use of manned mini-submarines or submersible vehicles for covert actions. Analysts seem to believe that China’s nuclear attack submarine technology lags behind Russia and even further behind the United States (Hampel 2018), but this push for modernization is a worrying trend in terms of securing UCCI. China already has unmanned undersea vehicles, remote operated vehicles, and autonomous undersea vehicles that are used for everything from sonar countermeasures to resource extraction (Goldstein 2017). China’s Underwater Great Wall Project is a submerged sensor network to monitor underwater activity in the South China Sea (Bana 2016; Trevithick 2017). One rationale for the project is the belief that China’s lack of monitoring ability is not commensurate with “the growing strategic threat” (Goldstein 2016). The network uses fiber-optic cables to send high-definition real-time data to manned and unmanned surface ships and employs remote operated vehicles to manipulate the deployment and configuration of underwater sensors, associated equipment, and cables (Sutton 2018). Even though Chinese remote operated vehicles can manipulate cables underwater, whether China can tap undersea cables is not yet known. Still, with the technology China has amassed, it is probable they can tap cables from surface ships or undersea vehicles, if not yet from submarines. On the whole, China’s rise and military modernization equates to China having the strategic interest and technological means to undermine Korea’s communications infrastructure if it so desires.

Japan and North Korea seem like almost polar opposites when it comes to submarine fleets and capabilities. The Japanese submarine fleet is highly sophisticated with some of the best trained crews in the world (Japan Times 2015). The North Korean submarine fleet is numerically the largest in the world (GFP 2019), but its quality and capabilities are far behind the major powers. The Japanese navy does have a deep-sea rescue vehicle, unmanned submersibles, and is intent on developing underwater drones for monitoring remote islands and possibly conducting surveillance (Burke and Ichihashi 2018; Rogoway 2019). The deep-sea rescue technology is certainly capable of manipulating cables on the seafloor and Japanese companies are intimate with undersea fiber-optic cables as they make and deploy that technology. The North Koreans
may not be able to manipulate cables yet, but twenty years ago a North Korean submarine suspected of spying was sunk one hundred kilometers south of Koeje Island (BBC 1998). The area of the sinking is the transit pathway to the greater Pacific for South Korea’s undersea cables. It is just one such submarine intrusion in South Korean waters over the years.

**CYBER CAPABILITIES OF REGIONAL THREAT ACTORS**

The final security issue to be discussed is the threat of cyber aggression against South Korea’s UCCI. In the simplest terms, the nightmare scenario is a hacker breaching the presentation server of a network management system (Sechrist 2012, 13-14). The presentation server is the graphical user interface that shows the system’s web-based applications and system equipment. Depending on the network management system, the hacker may gain access to multiple cable management systems with the ability to divert data traffic or delete/drop fiber wavelengths on one or more cable systems. These are just two of the potential system changes that could be enacted. Such aggressions are made easier as network management systems are typically web-based systems with internet connectivity made to run on Windows operating systems (see Sechrist 2012, 18-21, for an easy to understand breakdown of the vulnerabilities of three management systems).

The worry for South Korea is that China, Russia, and North Korea have sophisticated state-sponsored cyber aggression programs that target complex systems. Of the twenty advanced persistent threats (APTs)—groups that receive direction and support from an established nation state—tracked by FireEye (2019), thirteen are attributed to China, and two each to Russia and North Korea. In fact, Russia, China, North Korea, South Korea, and Japan are all recognized as cyber heavyweights by cyber security experts, with Russia and China ranked first and second respectively among states in overall cyber capabilities (Maness and Valeriano 2015, 92-93). North Korea and South Korea tied for fifth behind Israel and the United States, which had the highest level of offensive cyber capabilities, and Japan brings up the tail end of the heavyweight class with France, India, and Pakistan (Clark and Knake 2010, chapter 4; ibid.).

When it comes to UCCI and South Korea’s cables in particular, Japan may add to its heavyweight credentials as the Japanese companies NEC, Fujitsu, and KDD-SCS have provided equipment and network systems on four of South Korea’s six largest cables by data throughput (STF Analytics 2018). Familiarity with these systems may provide Japan an advantage in potential cyber aggressions against South Korea’s UCCI.

In their study of cyber conflicts between rivalry dyads, Valeriano and Maness
conclude the North Korea-South Korea dyad is third most active behind the China-US and Pakistan-India dyads, while the South Korea-Japan dyad is ranked fifth. Interestingly, when it comes to the South Korea-Japan dyad, both states seem to initiate incidents nearly equally (Valeriano and Maness 2014, replication dataset). Regarding the North Korea-South Korea dyad, attacks on South Korea’s defense data center, Ministry of Defense, defense industry firms, Korea Hydro and Nuclear Power, and banking infrastructure, as well as attacks on the SWIFT financial network, other financial institutions, cryptocurrency exchanges, the United Nations, and Sony Pictures have all been attributed to North Korea (CSIS 2019; Lee and Lim 2016; Nichols 2019). It is believed that North Korea’s Reconnaissance General Bureau runs Unit 180 for hacking financial institutions and the state has a Strategic Cyber Command responsible for other aggressions (Park and Pearson 2017). FireEye (2019) believes that South Korea is the primary target of APT37, attributed to North Korea. The group targets “various industry verticals, including chemicals, electronics, manufacturing, aerospace, automotive, and healthcare.”

China’s cybersecurity and cyber aggression policymaking system is considerably complex, but at the center are a number of Chinese Communist Party groups including the Cybersecurity and Informatization Leading Group chaired by President Xi Jinping (for a detailed view of Chinese cyber operations see Lindsay, Cheung and Reveron 2015). The group APT10, supported by China’s Ministry of State Security has been “targeting healthcare, defence, aerospace, government, heavy industry and mining” as well as companies in the US utilities sector (Majumder 2019; NCSC 2018). China has also been accused of trying to hack into South Korean embassy and military networks in 2008 (CSIS 2019), along with other aggressions toward South Korean targets. As of now, no cable system landing in South Korea is configured using equipment from the Chinese company Huawei. Huawei has the distinction of being the only submarine cable equipment manufacturer accused of espionage on behalf of a state. The suspicions and accusations have been ongoing for years (see Carroll 2017; Jung 2018; Shu 2018). For South Korea, these concerns should be palpable, as Huawei is a leader in submarine cable management equipment and cable system operations and therefore likely has great familiarity with the systems built by their competitors.

Unlike China and Japan, Russia does not have a private or state-supported company that is a major supplier of undersea cable systems equipment. However, like China and North Korea, Russia has a well documented history of cyber aggressions against complex systems, though South Korea does not appear to be a frequent target of these aggressions. There is little doubt that Russia has
the capability to perform disruptive cyber aggressions against South Korea’s UCCI. Russian hackers have been accused of targeting and or penetrating European government agencies, Indonesia’s voter database, the US Democratic National Committee, the US Securities and Exchange Commission, government agencies of NATO members, the Czech foreign ministry, and much more (CSIS 2019). With such powerful cyber actors in Northeast Asia, South Korea’s UCCI may be an enticing target in times of conflict or tension.

CONCLUSIONS AND RECOMMENDATIONS

Tsuruoka (2018) has called undersea communications cables the Achilles’ heel in a coming new cold war. He rightly notes three important facts about threats and vulnerability: 1) a foe’s hostile act on undersea cables could blind a country’s military, diplomatic, and economic communications; 2) the weapons for such acts will include submarines, underwater drones, robots, specialized ships, and divers; and 3) China, Russia, the United States, and others are focusing on “these deep-sea information pipes as rich sources of intelligence as well as targets in war.” It is no wonder then that twenty-four percent of US overseas CIKR is cable landings, including four landings at three different locations in South Korea. Protection of this undersea critical infrastructure will be paramount in future conflicts.

It is almost impossible to overstate the importance of and South Korea’s reliance upon this critical infrastructure for security and stability. South Korea is a state with no terrestrial telecommunications links to the greater Asian continent and therefore relies almost wholly upon its UCCI for all international communications. Nevertheless, the importance of this CI seems underappreciated by the South Korean government. The state has no comprehensive definition of a threat to CI and no definition of threat codified in law where UCCI is concerned. In addition, the state requires design basis threat analysis for nuclear power plants but has no such requirement for UCCI, leaving threat or vulnerability analyses up to the responsible administrative body. Furthermore, unlike US CIKR designations, South Korea designates only one of four cable landing stations as critical infrastructure, which shows a remarkable degree of incongruity between these military alliance partners.

A DBT analysis shows South Korea is surrounded by regional state actors—China, Russia, North Korea, and Japan—with the motivations and capabilities to undertake aggressions against its UCCI. This does not mean these aggressions are imminent or even likely, but the potential exists for these actors to cause
serious harm to South Korea’s communications lifeline. Therefore, protection of this infrastructure cannot and should not be left solely to the private owners and operators of these transnational cable systems. There are a number of actions the government of South Korea can take to better prepare for potential aggressions against UCCI.

Firstly, the South Korean government should take a number of legislative steps. It should codify into law comprehensive definitions of threat and risk. It should designate all cable landing stations and cable systems as CI and grant one administrative entity the authority to take control of CI in times of aggression. This would align better with US CIKR designations and create security efficiencies. The government should also require a DBT analysis and vulnerability analysis of designated CI every few years, at minimum.

Secondly, monitoring and maintenance of submarine cables are performed by owners of those systems or by privately contracted parties. South Korea is much too reliant on UCCI to leave the majority of monitoring to the private sector. Publicly available information shows KT Corporation’s protection efforts during cable operations include a patrol boat (of fifty-five kilometer coverage), radar (with fifty kilometer visibility), and GPS alarm devices (KT Corporation 2009). Knowing the myriad of ways submarines, surface ships, unmanned vehicles, and divers can damage cables and disrupt communications, it seems reasonable that the government deploy underwater sensor networks and unmanned autonomous vehicles or remote operated vehicles to monitor cable integrity and threats. These should be operated by the South Korean navy or coast guard. Such a step in additional protection seems only prudent for two reasons: 1) the cable chokepoint in the Korea Strait is very narrow and shallow, which makes the cables an easy target, and 2) South Korea’s newly acquired F-35 combat aircraft require constant, international data connectivity. North Korea has already threatened to develop special armaments to destroy the aircraft (Smith 2019), but targeting submarine cables may be easier.

Thirdly, as cables are retired and replaced by new systems, South Korea should offer to fund and build underground facilities for cable landing stations and network operations centers (O’Malley 2019, 324). This would of course depend on engineering feasibility, but better protection for onshore physical facilities is necessary. The South Korean government should also consider funding all or part of a direct cable linking South Korea to its alliance partner the United States. This would be difficult to fully protect across the Pacific Ocean, but it would be the only cable with no facilities on the territories of Northeast Asian neighbours.

Lastly, South Korean authorities should work with cable owner/operators
to minimize the use of web-based management systems and minimize remote access to cable system equipment. The fact is that UCCI are the backbone of internet communications traffic and are therefore vulnerable to cyber breaches. Any network attached to the Internet is open to attack and a breach will likely occur. Implementing security protocols, like access to applications using biometric data, should be encouraged. If needed, the government can sponsor research and development efforts by the private sector to upgrade management system software security.

State actors in Northeast Asia have the motivations and capabilities to disrupt South Korea’s undersea communications. Undersea cables, onshore cable landing stations, and network operations centers are all vulnerable to the threats these actors pose. Although no aggression is imminent, the South Korean government should prepare for the worst, as their society is increasingly dependent on this critical infrastructure.

REFERENCES

**Act on Measures for the Protection of Nuclear Facilities, etc. and Prevention of Radiation Disasters** [원자력시설 등의 방호 및 방사능 방재 대책법] Act No. 15280, Enforcement Date: June 20, 2018. Accessed at http://www.law.go.kr/ (July 8, 2019).

**Act on the Protection of Information and Communications Infrastructure** [정보통신기반 보호법] Act No. 15376, Enforcement Date: May 22, 2018. Accessed at http://www.law.go.kr/ (July 7, 2019).

Associated Press, The. 2005. “New Nuclear Sub is Said to Have Special Eavesdropping Ability.” *The New York Times* (February 20). Accessed at https://www.nytimes.com/2005/02/20/politics/new-nuclear-sub-is-said-to-have-special-eavesdropping-ability.html (July 29, 2019).

Bak, Jongjae and Sangho Lee. 2017. “Koreas SecurityStrategic Capabilities to Counter Cyber Attack and Future Challenges” [사이버 공격에 대한 한국의 안보전략적 대응체계와 과제] *The Journal of Political Science and Communication* 20(3), 79-113.

Bana, Sarosh. 2016. “China’s Underwater Great Wall: Subsurface Sensors Give Beijing the Drop on South China Sea Challengers.” *The Washington Times* (August 30). Accessed at https://www.washingtontimes.com/news/2016/aug/30/chinas-underwater-great-wall/ (July 29, 2019).

Bank for International Settlements. 2019. “Consolidated Positions on Counterparties Resident in Korea.” Accessed at https://stats.bis.org/
BBC. 1998. “World: Asia-Pacific Sinking Sparks ‘Spy Sub’ Alert.” BBC News (December 18). Accessed at http://news.bbc.co.uk/2/hi/asia-pacific/237520.stm (August 4, 2019).

Birnbaum, Michael. 2017. “Russian Submarines Are Prowling around Vital Undersea Cables. It’s making NATO Nervous.” The Washington Post (December 22). Accessed at https://www.washingtonpost.com/ (July 27, 2019).

Blum, Andrew. 2012. Tubes: A Journey to the Center of the Internet. New York: Harper Collins Publishers Inc.

Broadband Commission for Sustainable Development. 2018. The State of Broadband: Broadband Catalyzing Sustainable Development. Geneva, Switzerland: International Telecommunication Union.

Burke, Matthew M. and Aya Ichihashi. 2018. “Japan to Develop Underwater Drone to Defend Remote Islands Against Chinese.” Stars and Stripes (November 6). Accessed at https://www.stripes.com/news/japan-to-develop-underwater-drone-to-defend-remote-islands-against-chinese-1.555374 (August 4, 2019).

Byrne, Leo. 2015. “N. Korea, Russia Sign Military Agreement.” NK News (November 13). Accessed at https://www.nknews.org/2015/11/n-korea-russia-sign-military-agreement/ (July 29, 2019).

Carroll, Michael. 2017. “Huawei, South Korea 5G Deal Worries US Politicians.” Mobile World Live (March 13). Accessed at https://www.mobileworldlive.com/featured-content/top-three/huawei-south-korea-5g-deal-worries-us-politicians/ (July 29, 2019).

Carter, Lionel, Douglas Burnett, Stephen Drew, Graham Marle, Lonnie Hagadorn, Deborah Bartlett-McNeil, and Nigel Irvine. 2009. Submarine Cables and the Oceans—Connecting the World. UNEP-WCMC Biodiversity Series No. 31. Accessed at https://www.unep-wcmc.org/resources-and-data/submarine-cables-and-the-oceans--connecting-the-world (July 20, 2019).

Chalfant, Morgan, and Olivia Beavers. 2018. “Spotlight Falls on Russian Threat to Undersea Cables.” The Hill (June 17). Accessed at https://thehill.com/policy/cybersecurity/392577-spotlight-falls-on-russian-threat-to-undersea-cables (June 19, 2018).

Chesnoy, José. 2016. “Presentation of Submarine Fiber Communication.” In José Chesnoy ed., Undersea Fiber Communications Systems, 2nd ed, London, UK: Academic Press/Elsevier, 3-19.

Choi, Jisun. 2019. “China’s Defense White Paper Makes Mention of THAAD
Assessing Threats to South Korea’s Undersea Communications Cable Infrastructure

Deployment in S. Korea.” *The Dong-A Ilbo* (July 25). Accessed at http://www.donga.com/en/article/all/20190725/1799470/1/China-s-defense-white-paper-makes-mention-of-THAAD-deployment-in-S-Korea (July 26, 2019).

Clark, Bryan. 2016. “Undersea Cables and the Future of Submarine Competition.” *Bulletin of Atomic Scientists* 72(4), 234-237. Accessed August 15, 2018. doi: 10.1080/00963402.2016.1195636.

Clarke, Richard A. and Robert K. Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do about It*. Australia: HarperCollins e-books.

Coates, Peter. 2015. “Undersea Cable Cutting History.” *Submarine Matters* (October 29). Accessed at https://gentleseas.blogspot.com/2015/10/undersea-cable-cutting-for-dummies.html (July 27, 2019).

CSIS. 2019. “Significant Cyber Incidents.” Center for Strategic and International Studies. Accessed at https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents (August 10, 2019).

Dacom Crossing, INFRA, Cable Landing Station. Accessed at http://www.dacomcrossing.co.kr/en/sub02/03.php (February 9, 2019).

Databank. 2019a. “Exports of Goods and Services (% of GDP).” World Development Indicators. World Bank Group. Accessed at https://databank.worldbank.org (February 5, 2019).

Databank. 2019b. “GDP (current US$).” World Development Indicators. World Bank Group. Accessed at https://databank.worldbank.org (February 5, 2019).

Davenport, Tara. 2015. “Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis.” *Catholic University Journal of Law & Technology* 24(1), 57-109.

Defense-Aerospace.com. Editor’s Note. Accessed at http://www.defense-aerospace.com/article-view/release/188968/vulnerable-undersea-cables-are-major-risk-for-western-defense%3A-report.html (August 3, 2019).

Department of Homeland Security. 2018. *Joint National Priorities for Critical Infrastructure Security and Resilience*. Accessed at https://www.dhs.gov/publication/joint-national-priorities (July 3, 2019).

DHS Office of Risk Management and Analysis. 2011. *The Strategic National Risk Assessment in Support of PPD-8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation*. Washington: Department of Homeland Security. Accessed at https://www.dhs.gov/
strategic-national-risk-assessment-snra (May 29, 2019).

FireEye. 2019. “Advanced Persistent Threat Groups.” Accessed at https://www.fireeye.com/current-threats/apt-groups.html (November 13, 2019).

GFP. 2019. “Total Submarine Strength by Country.” GlobalFirepower.com. Accessed at https://www.globalfirepower.com/navy-submarines.asp (August 4, 2019).

Goldstein, Lyle J. 2016. “China’s ‘Undersea Great Wall’.” The National Interest (May 16). Accessed at https://nationalinterest.org/feature/chinas-undersea-great-wall-16222 (August 3, 2019).

______. 2017. “America May Soon Find Itself in an Underwater War with China.” The National Interest (July 24). Accessed at https://nationalinterest.org/feature/america-may-soon-fight-itself-underwater-war-china-21650 (August 3, 2019).

Hampel, Alex. 2018. “The Rise of the People’s Liberation Army Navy: Chinese Naval Modernization from 1990 to 2018.” WhiteFleet.net (March 25). Accessed at https://whitefleet.net/2018/03/25/the-rise-of-chinas-peoples-liberation-army-navy-modernization-from-1990-to-2018/ (August 1, 2019).

Hilbert, Martin. 2015. “Big Data for Development: A Review of Promises and Challenges.” Development Policy Review 34(1), 135-174.

Hong, Junho. 2019. “Research on the Necessity of Cyber Security Control Tower” [사이버보안 컨트롤타워 필요성에 관한 연구]. Law Review (법학연구) 19(1), 235-254.

Hudson, John, and Ellen Nakashima. 2019. “Russia Secretly Offered North Korea a Nuclear Power Plant, Officials Say.” The Washington Post (January 29). Accessed at https://www.washingtonpost.com/world/national-security/russia-secretly-offered-north-korea-a-nuclear-power-plant-officials-say/2019/01/29/d1872588-a99b-4b68-ba34-9ce1bc95b573_story.html?utm_term=.a41ecf1fee3f7 (May 5, 2019).

International Atomic Energy Agency. 2009. “Development, Use and Maintenance of the Design Basis Threat: Implementing Guide.” IAEA Nuclear Series No. 10. Vienna: International Atomic Energy Agency.

International Telecommunication Union. 2017. Measuring the Information Society Report 2017, Volume 1. Geneva, Switzerland: printed by author.

Japan Times. 2015. “Japan’s Crack Submarine Fleet.” Japan Times (November 26). Accessed at https://www.japantimes.co.jp/opinion/2015/11/26/commentary/japan-commentary/japans-crack-submarine-fleet/#.XUaOoG5uJ9A (August 4, 2019).
Jo, Herim. 2019. “KADIZ Emerges as Potential Flash Point?” *The Korea Herald* (July 24). Accessed at http://www.koreaherald.com/view.php?ud=20190724000769 (July 25, 2019).

JoongAng Ilbo. 2019. “Tensions Rising.” *JoongAng Ilbo* (July 24). Accessed at http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=3065875 (July 25, 2019).

Jung, Damin. 2019. “Military Surveillance Questioned after North Korean Ship Drifts to Samcheok.” *The Korea Times* (June 19). Accessed at http://www.koreatimes.co.kr/www/nation/2019/06/205_270910.html (June 20, 2019).

Jung, Minho. 2018. “Korea Right to be Cautious about Huawei as Security Threat: Experts.” *The Korea Times* (September 3). Accessed at https://www.koreatimes.co.kr/www/tech/2018/09/133_254927.html (October 4, 2018).

Khalizad, Zalmay M. 1999. “Defense in a Wired World: Protection, Deterrence, and Prevention.” In Zalmay M. Khalizad and John P. White eds., *The Changing Role of Information Warfare*, Santa Monica, CA: RAND, 403-437.

Kim, Minwook. 2019. “NIS, Police Nab an Alleged Spy Sent by North.” *JoongAng Ilbo* (July 26). Accessed at http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=3065992 (July 27, 2019).

Korea Hydrographic and Oceanographic Agency. 2011. *East Sea and Yellow Sea [Map No. 849 – WGS-84]*. Republic of Korea: Ministry of Oceans and Fisheries.

Korea Internet Security Agency. 2015. *A Comparative Law Study on the Cybersecurity Response System*[사이버보안체계 강화를 위한 정보보호법제 비교법연구]. KISA-WP-2015-0042. December 한국인터넷진흥원.

KT Corporation. 2009. “Submarine Cable Protection in Korea.” Paper presented at the Asia-Pacific Economic Cooperation Workshop and Information Sharing on Submarine Cable Protection, Singapore, April 13. doc: 2009/TEL39/SPSG/WKSP/006.

Lee, Kyung-bok and Jong-in Lim. 2016. “The Reality and Response of Cyber Threats to Critical Infrastructure: A Case Study of the Cyberterror Attack on the Korea Hydro & Nuclear Power Co., Ltd.” *KSII Transactions on Internet and Information Systems* 10(2), 857-880.

Lindsay, John R., Tai Ming Cheung and Derek S. Reveron. 2015. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford: Oxford University Press.

LIRNEasia. 2007. “Vietnam’s Submarine Cable ‘Lost’ and ‘Found’.” LIRNEasia,
General (June 2). Accessed at https://lirneasia.net/2007/06/vietnams-submarine-cable-lost-and-found/ (July 25, 2019).

Lukin, Artyom. 2016. “Russia’s Role in the North Korea Conundrum: Part of the Problem or Part of the Solution?” [E-Notes] Foreign Policy Research Institute (March 4). Accessed at https://www.fpri.org/article/2016/03/russias-role-in-the-north-korea-conundrum-part-of-the-problem-or-part-of-the-solution/ (May 3, 2019).

MacAskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies, and James Ball. 2013. “GCHQ Taps Fibre-Optic Cables for Secret Access to World’s Communications.” The Guardian (June 21). Accessed at https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (October 5, 2018).

Majumder, Bhaswati Guha. 2019. “Chinese State-Backed Hackers APT10 Behind Cyber Attack on US Utilities?” International Business Times (August 3). Accessed at https://www.ibtimes.sg/chinese-state-backed-hackers-apt10-behind-cyber-attack-us-utilities-31973 (August 10, 2019).

Maness, Ryan C. and Brandon Valeriano. 2015. Russia’s Coercive Diplomacy: Energy, Cyber and Maritime Policy as New Sources of Power. UK: Palgrave Macmillan.

Marks, Paul. 2013. “Submarine Internet Cables are a Gift for Spooks.” NewScientist (June 25). Accessed at https://www.newscientist.com/article/dn23752-submarine-internet-cables-are-a-gift-for-spooks/ (November 2, 2018).

Matsakis, Louise. 2018. “What Would Really Happen if Russia Attacked Undersea Internet Cables.” Wired.com (January 5). Accessed at https://www.wired.com/story/russia-undersea-internet-cables/ (November 2, 2018).

Ministry of Science, ICT and Future Planning. 2013. National Cyber Security Comprehensive Countermeasures [정부, 국가 사이버안보 중합대책 수립: 사이버안보 강화를 위한 4대 전략(PCRC) 마련]. Seoul: 미래창조과학부.

______. 2015. National Critical Infrastructure Designation [국가기반시설 지정]. Notice 2015-73 (제2015-73호).

Mizokami, Kyle. 2017. “How a Super-Secret U.S. Navy Submarine Tapped Russia’s Underwater Communications Cables.” The National Interest (June 29). Accessed at https://nationalinterest.org/blog/the-buzz/how-super-secret-us-navy-submarine-tapped-russias-underwater-21370 (July 25, 2019).
Nagpal, Vinay. 2018. “Virginia: the Data Center Capital of the World is Now at the Confluence of Five Continents.” *Global Capacity* (Issue 100), May, 26-29. Accessed at https://subtelforum.com/products/subtel-forum-magazine/ (July 7, 2018).

*National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency.* 2009. Washington: Department of Homeland Security.

National Security Office. 2019. *National Cybersecurity Strategy* [국가 사이버안보 전략]. Seoul: 청와대.

NCSC. 2018. “APT10 Continuing to Target UK Organisations.” National Cyber Security Centre, United Kingdom (December 20). Accessed at https://www.ncsc.gov.uk/news/apt10-continuing-target-uk-organisations (August 10, 2019).

Nichols, Michelle. 2019. “North Korea Took $2 billion in Cyberattacks to Fund Weapons Program: U.N. Report.” Reuters (August 6). Accessed at https://www.reuters.com/article/us-northkorea-cyber-un-idUSKCN1UV1ZX (August 10, 2019).

Office of the Secretary of Defense. 2017. *Military and Security Developments involving the People’s Republic of China 2017* (Annual Report to Congress). May 15. Washington, DC: United States Department of Defense.

Oh, Seok-min. 2019. “N. Korea Fires 2 Short-Range Missiles into East Sea: JCS.” *Yonhap News* (July 25). Accessed at https://en.yna.co.kr/view/AEN20190725000855325?section=national/defense (July 26, 2019).

O’Malley, Sean. 2019. “Vulnerability of South Korea’s Undersea Cable Communications Infrastructure: A Geopolitical Perspective.” *Korea Observer* 50(3), 309-330.

Osborn, Andrew and Joyce Lee. 2019. “First Russian-Chinese Air Patrol in Asia-Pacific Draws Shots from South Korea.” *Reuters* (July 23). Accessed at https://uk.reuters.com/article/uk-southkorea-russia-aircraft/first-russian-chinese-air-patrol-in-asia-pacific-draws-shots-from-south-korea-idUKKCN1UI06X (July 24, 2019).

Park, Ju-min and James Pearson. 2019. “Exclusive: North Korea’s Unit 180, the Cyber Warfare Cell that Worries the West.” *Reuters* (May 21). Accessed at https://www.reuters.com/article/us-cyber-northkorea-exclusive-idUSKCN18H020 (August 10, 2019).

Presidential Decree 28211, pertaining to the *Act on Measures for the Protection of Nuclear Facilities, etc. and Prevention of Radiation Disasters* [원자력시설 등의 방호 및 방사능 방재 대책법 시행령] Enforcement Date: July 26, 2017. Accessed at http://www.law.go.kr/ (July 4, 2019).
Presidential Decree 29421, pertaining to the *Act on the Protection of Information and Communications Infrastructure Enforcement Decree* [정보통신기반 보호법 시행령] Enforcement Date: January 1, 2019. Accessed at http://www.law.go.kr/ (July 7, 2019).

Reichmann, Deb. 2018. “Could Enemies Target Undersea Cables that Link the World?” *The Associated Press* (March 31). Accessed at https://apnews.com/c2e7621bda224e2db2f8c654c9203a09 (October 9, 2019).

Risk Steering Committee. 2010. *DHS Risk Lexicon*, 2010 edition. Washington: Department of Homeland Security.

Robinson, Neil, Luke Gribbon, Veronika Horvath, and Kate Robertson. 2012. *Cyber-security Threat Characterisation: A Rapid Comparative Analysis*. n.l.: RAND Europe.

Rogoway, Tyler. 2019. “Here’s Everything We Know about the Ongoing Search for Japan’s Crashed F-35 (updated).” *The War Zone* (April 13). Accessed at https://www.thedrive.com/the-war-zone/27428/heres-everything-we-know-about-the-ongoing-search-for-japans-crashed-f-35 (August 4, 2019).

Sechrist, Michael. 2012. *New Threats, Old Technology: Vulnerabilities in Undersea Communications Cable Network Management Systems*. Discussion Paper No. 2012-03, Cambridge, MA: Harvard Kennedy School, Belfer Center.

Sechrist, Michael, C. Vaishnav, D. Goldsmith, and Nazli Choucri. 2012. “The Dynamics of Undersea Cables: Emerging Opportunities and Pitfalls.” Paper presented under the title “The Dynamics of Undersea Cables: Can the Old Modes of Governance Cope with New Demands of the Cyberspace?” at the 30th International Conference of the System Dynamics Society, St. Gallen, Switzerland, July. Accessed at https://ecir.mit.edu/publications/conference-proceedings (July 19, 2018).

Seidel, Jamie. 2019. “‘Catastrophic’ Risk Run by Doomed Russian Nuclear Submarine,” *News Corp Australia* (July 10). Accessed at https://www.news.com.au/technology/innovation/military/mysterious-mission-of-doomed-russian-nuclear-submarine/news-story/b1dac3461c5367d42e7cf4d0e2a088b (July 25, 2019).

Shu, Catherine. 2018. “New Defense Bill Bans the U.S. Government from Using Huawei and ZTE Tech.” *Techcrunch* (August 13). Accessed at https://techcrunch.com/2018/08/13/new-defense-bill-bans-the-u-s-government-from-using-huawei-and-zte-tech/ (October 20, 2018).

Smith, Josh. 2019. “North Korea calls South Korea’s F-35 jet purchases ‘extremely dangerous action’.” *Reuters* (July 11). Accessed at https://
www.reuters.com/article/us-northkorea-southkorea-aircraft/north-korea-calls-south-koreas-f-35-jet-purchases-extremely-dangerous-action-idUSKCN1U60BJ (August 3, 2019).

Song, Sang-ho. 2019. “Amid Cross-Border Détente, S. Korea Confronts Potential Threats from Outside.” Yonhap News (March 6). Accessed at http://yna.kr/AEN20190305005100315 (July 25, 2019).

STF Analytics. 2018. Submarine Cable Almanac, Issue 26. Submarine Telecoms Forum. Accessed at https://subtelforum.com/ (July 27, 2018).

Sub marinenetworks.com. https://www.sub marinenetworks.com.

Sunak, Rishi, MP. 2017. Undersea Cables: Indispensable, Insecure. London, UK: Policy Exchange. Accessed at https://policyexchange.org.uk/publication/undersea-cables-indispensable-insecure/ (June 16, 2018).

Sutton, H. I. 2018. “Good Wind Ears: China’s Underwater Great Wall.” Covert Shores (May 27). Accessed at http://www.hisutton.com/Cn_Underwater_Great_Wall.html (August 3, 2019).

Szayna, T.S., Byman, D., Bankes, S. C., Eaton, D., Jones, S. G., Mullins, R., ... Rosenau, W. 2001. The Emergence of Peer Competitors: A Framework for Analysis. Santa Monica, CA: RAND Corporation.

TeleGeography. Submarine Cable Map. Accessed at https://www.submarinemap.com (May 15, 2019).

Trevithick, Joseph. 2017. “South China Sea Underwater ‘Environmental’ Sensor Net Could Track U.S. Subs.” The War Zone (May 30). Accessed at http://www.thedrive.com/the-war-zone/10906/south-china-sea-underwater-environmental-sensor-net-could-track-u-s-sub (September 10, 2018).

______. 2019. “North Korea’s New Ballistic Missile Submarine Is a Refurbished Antique (Updated).” The War Zone (July 23). Accessed at https://www.thedrive.com/the-war-zone/29122/north-koreas-new-ballistic-missile-submarine-is-a-refurbished-antique (July 24, 2019).

Tsuruoka, Doug. 2018. “Undersea Cables the Achilles’ Heel in Lead Up to New Cold War.” Asia Times (January 6). Accessed at https://www.asiatimes.com/2018/01/article/undersea-cables-achilles-heel-lead-new-cold-war/?_=3105948 (June 16, 2018).

United States Office of the Director of National Intelligence. 2017. Threats to Undersea Cable Communications. September. Accessed at https://www.dni.gov/files/PE/Documents/1---2017-AEP-Threats-to-Undersea-Cable-Communications.pdf (July 9, 2018).

Valeriano, Brandon and Ryan C. Maness. 2014. “The Dynamics of Cyber
Conflict between Rival Antagonists, 2001-2011.” *Journal of Peace Research* 51(3), 347-360.
_______. 2014. “The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011.” *Journal of Peace Research* 51(3), Replication Dataset. Accessed at https://www.prio.org/jpr/datasets/#2014 (August 14, 2019).

WikiLeaks. 2010. Canonical ID: 09STATE15113_a. “Request for Information: Critical Foreign Dependencies (Critical Infrastructure and Key Resources Located Abroad.” United States Department of State, February 18, 2009. Accessed at https://www.wikileaks.org/plusd/cables/09STATE15113_a.html (July 13, 2019).

Winkler, Jonathan Reed. 2015. “Silencing the Enemy: Cable-Cutting in the Spanish-American War.” *War on the Rocks* (November 6). Accessed at https://warontherocks.com/2015/11/silencing-the-enemy-cable-cutting-in-the-spanish-american-war/ (July 25, 2019).

Xiong, Herbert. 2017. *Regional Subsea Cable System in Southeast Asia Region.* TE Subcom, September. Accessed at https://www.ptc.org/wp-content/uploads/2017/10/1-herbert-xiong-regional-submarine-cable-system-of-sea-market.pdf (July 29, 2019).

Yonhap News. 2019a. “Japanese Ambassador: Export Restrictions Due to ‘Collapse’ of Mutual Trust.” *Yonhap News* (July 8). Accessed at http://yna.kr/AEN20190708006700315 (July 10, 2019).

Yonhap News. 2019b. “S. Korea May Review Military Info-Sharing Pact with Japan: Cheong Wa Dae Official.” *Yonhap News* (July 18). Accessed at http://yna.kr/AEN20190718010251315 (July 19, 2019).

[Received Sep 21, 2019; Revised Oct 16, 2019; Accepted Nov 7, 2019]