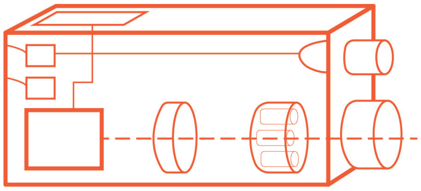

2 | Understanding Situational Awareness Technologies and the Emerging Situational Awareness Ecosystem

The rapid expansion of new and existing technologies can provide opportunities for major breakthroughs in the ability to detect threats; track hostile actions and forces; process, interpret and communicate vast data sets; and predict and shape the actions and possibly even decisions of adversaries. Every technology has costs and benefits associated with its adoption, and the capabilities in the emerging strategic SA ecosystem are no different. Each of the emerging capabilities explored over the course of this project can be described using two separate categories: attributes for increasing strategic SA (discussed in this chapter) and risk factors that decrease strategic stability (addressed in the next chapter).

Platforms, Critical Enablers, and Defense and Counter Capabilities

The new technologies that will shape the strategic SA ecosystem moving forward can be divided into several broad categories. For the purposes of understanding and analyzing SA technologies and their effect on strategic stability, this study draws a distinction between "platforms" and "critical enablers." "Platforms," such as satellites, unmanned aerial vehicles (UAVs) or unmanned underwater vehicles (UUVs), or even microchip-enabled proximity cards, are the physical systems or structures necessary to access a collection target, carry a variety of sensor payloads, and support communications and data transmission from the sensor package. "Critical enablers," on the other hand, are the sensors, applications, or other technologies used to collect or analyze SA data many of which can be used on or in support of a variety of platforms. In the examples above, these would be the sensors attached to a UAV or the digital applications which collect and analyze data collected by those sensors. Technological advancement and innovation have been key to the development of both platforms and critical enablers. For example, advances in miniaturization, autonomy, robotics, and other technologies have led to the development of platforms that are smaller, more mobile and agile, and harder to detect. To better analyze the individual technology and the costs and benefits associated with employing it, platforms and critical enablers may be treated as a distinct for academic or theoretical purposes. However, in real-world scenarios, a critical enabler is useful only after its marriage with a platform that can put it into position to gather and process desired information.

Finally, in addition to platforms and critical enablers, this project also explored some strategic SA capabilities that may be termed “defense” or “countering.” These capabilities contribute to the strategic SA ecosystem differently than most platform-critical enabler combinations: whereas most strategic SA capabilities focus on collecting information that can be used to inform decisionmakers during crisis or conflict, defense and countering capabilities either defend against adversary activities (for example, cognitive electronic warfare systems tasked with detecting, suppressing, and neutralizing adversary cyber intrusions) or seek to counter or degrade an adversary’s strategic SA (such as through spoofing activities that can obfuscate an adversary’s ability to perceive the operating environment). Together, defense and countering capabilities account for a small number of capabilities explored during this project, but such technologies may play an outsized role in escalation dynamics during future crises or conflicts given their potentially destructive nature and relevance to gray zone tactics.[1]

Key Attributes of Strategic SA Capabilities

To facilitate comparative analysis of a wide variety of technical capabilities and understand the enhancements they bring to strategic SA, the study team developed a common set of criteria or beneficial attributes that contribute to a highly effective strategic SA ecosystem. The six technical attributes are: vantage/range, speed, detectability, precision, persistence, and resiliency/reliability. Figure 2.1 defines each of these attributes and offers an example of a technical capability in which that attribute figures prominently.

VANTAGE AND RANGE

Vantage and range address the position within the physical operating environment from which new information can be gathered. While vantage focuses on the position from which information can be gathered (i.e., the position of the technology relative to the target being surveilled), range indicates

Figure 2.1 Emerging Technology Attributes

ATTRIBUTES

ATTRIBUTES	DEFINITION	TECHNOLOGY EXAMPLES
Vantage/ Range	*The position from which new information can be ascertained.*	*Pseudosatellites that can position highly capable sensors outside of targetable distance.*
Speed	*The shortening of time between an adversary’s action or decision to act, detection of that action, and the receipt of such by decision-makers.*	*Quantum computing that accelerates the ability to process and analyze vast data sets.*
(Un)detectability	*The degree to which an adversary can ascertain that information is being collected.*	*Advanced stealth capabilities that allow sensor platforms to evade detection by adversary air defenses.*
Precision	*The level of detail and quality of the information collected or a heightened degree of confidence in the information collected.*	*Synthetic Aperture Radar (SAR) that can track military movements despite weather and cloud cover.*
Smallsat	*The extent to which the capability can continuously collect data without gaps in coverage.*	*SmallSat constellations that can surveil specific areas for weeks or months.*
Resiliency/ Reliability	*The ability of a technology to employ redundant and robust systems for situational awareness in a contested environment.*	*Multi-sensor payload UAV swarms that can operate even if some of the platforms are destroyed or disabled.*

the operational "field of view" of the technology (i.e., the distance over which the capability can provide insight).

Some capabilities enable vantage benefits that were previously unattainable, inaccessible, or excessively costly or dangerous to attain. For example, high-altitude pseudosatellites provide a unique vantage to surveil adversaries, as their position between traditional UAVs and satellites provides a greater slant range without having to be directly over a target.[2] Elsewhere, plant-based sensors—an emerging SA technology that consists of physiology-based sensors capable of reporting the presence of various stimuli— could provide on-the-ground data collection that would otherwise require covert insertion, risky air drops, or other methods that could be considered violations of territorial integrity.[3] For example, these "smart plants" could be distributed either passively (e.g., via wind, wildfire, water, or animals) or actively (e.g., via mechanical or non-mechanical human activity).[4]

Range is related to vantage but refers specifically to the standoff distance afforded by the capability. Light Detection and Ranging (LIDAR) sensors can be calibrated to map ground structures through cloud cover using air or space assets that would have previously required flying at lower altitudes.[5] UUVs could be deployed inside safe territory and travel thousands of nautical miles to collect data.[6] China revealed its first large-displacement autonomous underwater vehicle (AUV), the HSU-001, in October 2019.[7] The U.S. Navy operates a limited number of UUVs primarily in a mine countermeasures (MCM) role, but it also has two major UUV developmental efforts underway: the Large Diameter UUV (LDUUV) and the Extra-Large UUV (XLUUV).[8] Both programs are still in early development and are not expected to shift to production until the mid-2020s.[9]

In any case, through enhanced range and vantage a state can optimize its ability to collect information at a distance, thereby minimizing risks of attack or sabotage to its own strategic SA assets.

SPEED

Whereas vantage and range denote a capability's advantageous position in space, speed refers to a capability's implications for time, namely the shortening of time between an adversary's action or decision to act, detection of that action, and the conveyance of information to the decisionmaker. Increased speed is a hallmark attribute of new technologies, driven by collectors' preferences for the rapid collection of more and more information to provide actionable options to decisionmakers.

> *Increased speed is a hallmark attribute of new technologies, driven by collectors' preferences for the rapid collection of more and more information to provide actionable options to decisionmakers.*

Computer technologies that focus on data collection, analysis, or decision support are particularly relevant for "speed" given their ability to execute processes, detect changes in adversary systems, analyze large quantities of data, and quickly transmit the information across networks. Cyber surveillance capabilities can perform a wide variety of tasks and collect information at speeds that were previously unattainable. For example, they can intercept military leadership communications about troop movements, thereby shortening the time it would take to otherwise detect such actions. AI decision-support applications and quantum computing are comparatively newer technologies but could radically increase the speed at which decisions can be made or detected.

AI analysis applications are an example of a capability's potential to increase speed across multiple levels of strategic SA, including data collection, analysis, and decision-support tools. AI pattern recognition applications could sift through large amounts of data, including video, imagery, signal intercepts, and technical intelligence collected by strategic SA assets, and flag items of interest for analysts, thereby reducing the amount of time needed to analyze complex situations.[10] While many speculate that China may be gaining an edge in AI,[11] various press reports suggest that the United States currently has several major AI programs in development, including Project Maven and a classified pilot program reported by Reuters in 2018 focused on tracking the North Korean nuclear missile program.[12] Project Maven, a high-profile U.S military program, reportedly aims to use AI and machine learning to help intelligence analysts identify objects of interest from both moving and still imagery generated by the Unmanned Aircraft Systems fleet.[13] Although the mission of the latter program is classified, it is believed to focus on leveraging AI to monitor the North Korean nuclear program using satellite imagery to track mobile launchers, which can be difficult for human analysts to locate and track in real time.[14] Moreover, while available sources suggest that technology in North Korea is well behind that of South Korea, its rapid advances in cyber operations and information and communications technology suggest that it can be anticipated in the near future to develop machine learning and other types of AI technology and to apply those technologies in military affairs.[15] In a crisis involving compressed timelines, speed can be essential— information that arrives too late might as well not arrive at all.

DETECTABILITY

Detectability is the degree to which adversaries can recognize and identify surveillance activities targeting them. Certain capabilities such as advanced stealth surveillance aircraft may facilitate data gathering at reduced risk of detection. For instance, the United States is reportedly developing the RQ-180 Sentinel, a low-observable, unmanned HALE aircraft likely capable of active and passive electronic surveillance and electronic attack.[16] UUVs are an example of a currently-detectable capability that, given potential evolutions in related technologies (e.g., miniaturization, stealth, and quieting technology) stand to become increasingly difficult to detect.[17] Low detectability increases the ability to survey a target without detection, thereby collecting valuable information without the adversary's knowledge.

Even if an intrusion is detected, attribution can be a challenge. For example, given the nature of computer architecture, an adversary may find a cyber surveillance vulnerability and detect (or assume) a cyber intrusion but still be unable to determine what data is being surveilled. Advances in quantum computing may create scenarios where cyber surveillance is undetectable: recent research has demonstrated successful cloning of qubits, which may allow for undetectable, non-destructive, and non-intrusive hacking of both traditional and quantum computer systems.[18] According to various reports, the Reconnaissance General Bureau (RGB), North Korea's intelligence service, operates a number of hacking groups for which governments and cybersecurity companies attribute a variety of names (e.g., APT 38, Lazarus Group, TEMP Hermit, Hidden Cobra, APT 37, Group 123, Nickel Academy, Guardians of Peace, Silent Chollima, and Reaper).[19] Recorded Future, a cybersecurity firm, analyzed internet activity from territorial North Korea and found that little to no malicious cyber activity emanated from the North Korean mainland during the period observed, suggesting that North Korean state-sponsored cyber operations originated from locations outside of territorial North Korea, such as India, Malaysia, New Zealand, Nepal, Kenya, and Indonesia.[20]

PRECISION

Precision is defined as the level of detail and quality of the information collected or a heightened degree of confidence in the information collected. This attribute is particularly relevant for remote sensing capabilities, as more precise or detailed information is often the differentiating factor from older-generation technologies (more detailed optical sensors that provide higher-resolution photographs, for example). Advances in sensor technologies improve not only collection methods but also improve the value of the data itself in some cases. Whereas most mapping assets are typically restricted to either precision or volume, LIDAR's higher spatial sampling frequency can be dynamically changed to improve map accuracy at the cost of a lower data collection rate (measured in square kms/hr).[21]

Synthetic Aperture Radar (SAR) has been a core element of U.S. satellite surveillance capabilities for years, but until recently, such sensors were unable to image moving targets. Over the past two decades, however, advances in data-processing techniques have enabled SAR to both detect moving targets and determine their speed and direction of travel.[22] News reports suggest that a Chinese satellite constellation, Yaogan, employs both optical and SAR sensors and involves more than 50 satellites.[23] These advanced precision upgrades to SAR make the collected information more detailed and can contribute toward achieving important operational and strategic tasks such as tracking mobile missiles.

PERSISTENCE

Persistence is the extent to which a capability can continuously collect data by avoiding gaps in coverage. Persistence provides decisionmakers with important information that can give a clearer picture of a crisis or conflict over time, with fewer gaps in coverage, which in turn can greatly increase confidence levels. For example, HALE UAV pseudosatellites rate favorably for persistence because they could be capable of staying aloft for over three weeks, continuously monitoring a specific target and transmitting data the entire time.[24]

Current capabilities employed by the United States and China that are relevant to persistence include traditional HALE UAVs, a capability that provides persistence (but to a lesser degree than the potential of future pseudosatellites). China's People's Liberation Army (PLA) Navy operates the BZK-005 HALE UAV for maritime surveillance in the East and South China Seas, the Xiang Long HALE UAV, which could presumably be used in support of airborne early warning, and others.[25] The United States operates an extensive fleet of HALE UAVs, including the RQ-4 Global Hawk and the RQ-180. The RQ-4 Global Hawk has high-altitude surveillance capabilities similar to other assets but importantly offers persistent surveillance, with the ability to loiter for more than 34 hours.[26]

UUVs could also provide persistence: after being deployed directly into contested waters, UUVs can lie dormant until "awoken" by passing submarines, enabling the monitoring of areas through a latent capacity that was previously unachievable.[27] While the United States could be considered at the forefront of deploying UUVs to track detected submarines, the Chinese Academy of Science is reportedly carrying out research on unmanned maritime vehicles (UMVs) as well.[28]

RESILIENCY AND RELIABILITY

Resiliency and reliability refer to the ability of a capability to employ redundant, robust systems in a contested environment. The presence of a "back up" reduces the chances that a capability will "fail" in collecting useful information. Similarly, redundant, "swarmed" capabilities can "flood the zone" and confound the adversary's ability to target or disable the capability even if detected.

The United States has multiple efforts underway to develop "swarming" capabilities in which small UAVs, numbering from just a few to potentially thousands, are networked together and share information to form the swarm's collective brain.[29] This collective brain then autonomously controls and directs the individual UAVs comprising the swarm in pursuit of the swarm's broader mission. If one or several drones are destroyed or debilitated, the swarm endures, as the collective brain compensates for the missing drones and then reorients. U.S. efforts to develop swarming capabilities are progressing along two main thrusts: disposable, air-launched micro-drones, which are roughly the size of a large hand, and small, reusable airborne UAVs which can be launched and recovered.[30] The effort to develop disposable, air-launched micro-drones, led by the Strategic Capabilities Office, successfully tested a swarm of 103 Perdix micro-drones in October 2016. Packed into flare canisters and ejected from an F/A-18 Super Hornet, the micro-drone swarm successfully "demonstrated advanced swarm behaviors such as collective decision-making, adaptive formation flying, and self-healing."[31]

Another form of resiliency can be seen in satellite constellations. Ranging from dozens to thousands, small satellite constellations improve the resiliency of the overall system to degradation due to natural causes, such as radiation damage, or adversary attacks.[32]

Surveying the Global Strategic SA Capabilities Landscape

Today, countries around the world possess varying degrees of strategic SA capabilities and continue to seek further advancements. The United States has extensive and mature strategic SA capabilities across all domains (air, land, maritime, space, and cyber) that help to characterize the operating environment, detect and respond to attacks, and discern actual attacks from false alarms across the spectrum of conflict, both conventional and nuclear. The U.S. military has always relied on these capabilities at the strategic level, but over the last 30-40 years, these capabilities have become more important at the tactical and operational level as technological advances have enabled more granular tracking and detection of enemy forces and communications, as well as coordination between different sensors and shooters, all with devastating effect. This combination of SA capabilities across all three levels of war and all domains has provided the United States unrivaled strategic SA and has become an essential component of U.S. military doctrine and planning. U.S. military superiority does not come from any stand-alone weapon system or platform, but its ability to integrate multiple C4ISR (command, control, communications, computers, information, surveillance, and reconnaissance) capabilities into a system-of-systems approach that translates strategic SA into kinetic and non-kinetic strike capabilities. The Navy's CEC/NFIC-CA capability is perhaps the best example of how several strategic SA systems, sensors, and platforms are integrated into a reconnaissance-strike complex with potentially devastating effect. If the United States wanted to target an adversary's capital ships—the most important ships in a fleet—it could send a stealthy F-35 to penetrate the enemy's air defense undetected and relay the enemy's location back to the carrier strike group; the strike group could then fire long-range anti-surface missiles at the enemy's capital ship without needing to get close.[33]

> *Military capabilities do not develop in a vacuum, and just as U.S. military planners recognized the value of integrating multiple systems, sensors, and platforms into a reconnaissance-strike complex, so too have American competitors.*

Northrop Grumman personnel conduct preoperational tests on a U.S. Navy X-47B Unmanned Combat Air System demonstrator aircraft on the flight deck of the aircraft carrier USS George H.W. Bush (CVN 77) May 14, 2013, in the Atlantic Ocean.

DoD photo by Mass Communication Specialist 2nd Class Timothy Walter, U.S. Navy/Released

Military capabilities do not develop in a vacuum, and just as U.S. military planners recognized the value of integrating multiple systems, sensors, and platforms into a reconnaissance-strike complex, so too have American competitors. The Chinese and Russians have developed sophisticated anti-access/area denial (A2/AD) capabilities that threaten to disrupt, degrade, or destroy essential U.S. C4ISR enabling capabilities. These advances are forcing military planners to rethink fundamental assumptions from the last 30 years about the near-guaranteed availability of C4ISR capabilities. Instead of establishing theatre-wide strategic SA superiority (e.g., U.S. operations in the 1991 Gulf War or Afghanistan and Iraq), the United States might only be capable of establishing temporary windows of C4ISR superiority for U.S. forces to operate from. U.S. military forces would work within these temporary windows of superiority to disintegrate enemy A2/AD systems and eventually re-establish theatre-wide strategic SA superiority, but this requires fundamental changes in U.S. training, doctrine, and force structures.[34]

China has invested and advanced considerably in its strategic SA capabilities. Although traditional shortcomings in its early-warning capabilities have been a major concern, the Chinese People's Liberation Army (PLA) today is poised to possess a more mature architecture that can enhance its capability to undertake nuclear counterattack and conventional operations. These range from space systems for electronic intelligence (ELINT) and remote sensing, including with aerial early-warning aircraft and unmanned systems, to a number of large, phased-array radars. In the years to come, China is likely to continue to redouble its efforts in response to new strategic requirements. For the PLA, the improvement of its capabilities for strategic early warning and SA will remain a challenge, but their efforts are starting to yield notable progress. Meanwhile, the PLA Rocket Force's new doctrinal emphasis on "rapid reaction" (快速反应) implies the capability for a rapid second strike, and China's posture could perhaps even evolve toward "launch on warning" (预警即发射), which would demand significantly more reliable early-warning systems. The expansion of this global architecture in the years ahead will likely remain a priority as the PLA seeks to enhance its capabilities for power projection and joint operations.[35]

As the Chinese military is tasked with becoming “world-class” by mid-century, continued advances in its capabilities could enable the PLA to leapfrog ahead of the United States in certain domains and technologies. Seeking to establish itself as an “aerospace superpower” (航天强国), China has launched a range of satellites at a rapid pace, quickly expanding its space-based surveillance capabilities, including its capacity to rapidly process and glean insights from that data. The PLA has also emerged as a clear leader in experimentation with the use of unmanned systems for early warning and reconnaissance, fielding and integrating a growing number of systems that could increase its flexibility in enhancing SA in a crisis or conflict scenario. Meanwhile, PLA cyber capabilities could also contribute significantly to Chinese espionage.[36]

> *The PLA has also emerged as a clear leader in experimentation with the use of unmanned systems for early warning and reconnaissance, fielding and integrating a growing number of systems that could increase its flexibility in enhancing SA in a crisis or conflict scenario.*

As the U.S.-China relationship becomes more competitive, even confrontational, these improvements in the PLA’s strategic SA capabilities could prove stabilizing in certain respects but may also create new risks and challenges. For instance, improved strategic early warning could decrease Chinese anxieties about the risks of a “false negative” and enable more time for decisionmaking in a crisis in ways that mitigate the risks of accidental escalation. However, continued improvement of Chinese strategic early warning over the next decade or more could facilitate a transition to a posture of launch on warning that could prove risky or destabilizing, particularly if this trend corresponds with an increased reliance on complex emerging technologies to support these missions, such as AI. At the same time, these increases in capabilities will also improve the PLA’s war-fighting capabilities in its near seas, including in likely conflict contingencies, while enabling future power projection. In this regard, these trends must be recognized as another dimension of China’s emergence as a rival that can challenge traditional U.S. technological leadership.[37]

Unclassified sources contain little information on North Korea’s C4ISR capabilities or strategic thinking. The country’s leadership has expressed interest in signals intelligence (SIGINT), electronic warfare (EW), and asymmetric warfare since at least the armistice of the Korean War, during which Kim Il Sung employed SIGINT and communications intelligence (COMINT) abilities within the Ministry of Internal Affairs and the Reconnaissance Bureau for use against both foreign and domestic enemies. In addition, open-source reports have detailed alleged incidents of North Korean GPS jamming and spoofing dating back to 2010. North Korea is known to use its GPS jamming capabilities against South Korea, disrupting air traffic at Incheon and Gimpo International Airports. According to a report, there were four GPS jamming and spoofing attacks tied to North Korea between 2010 and 2016.

North Korean cyberattacks have also grown in sophistication over the last decade. According to South Korean intelligence agencies, North Korean cyber operations between 2005 and 2007 mainly stole data and documents from South Korean government agencies through individual email accounts or agency websites. In 2005, the South Korean National Intelligence Agency found North Korean documents that ordered Lab 110 to "develop a hacking program to destroy the South's communication network and disguise the source of attack." These attacks were generally seen as rudimentary and simple. Since 2008, North Korea's cyberattack capabilities have started to focus on large-scale operations using complex malware. As North Korea's capabilities expanded, so did the range of targets: North Korean hackers have targeted government employees and institutions, researchers, cryptocurrency exchanges, banks, and media across the world. Until 2015, North Korean cyberattacks focused primarily on U.S. and South Korean government and financial organizations. However, in early 2016, North Korean hackers attempted to transfer $951 million from the Bangladesh Central Bank into North Korean-controlled accounts, the first of several subsequent North Korean attacks on banks around the world in 2017. American cybersecurity firm CrowdStrike assesses the speed of the North Korean hackers to be second only to Russian intrusion groups and superior to the Chinese.[38]

TWO STEPS FORWARD, ONE STEP BACK?

Emerging SA capabilities—characterized by the six attributes outlined above—will provide increased opportunities for strategic SA. Although the United States has traditionally been a frontrunner in SA capabilities, competitors such as China, Russia, and even North Korea are closing the gap. However, while these nascent capabilities may provide increased opportunities for strategic SA, they may also pose inadvertent risks to strategic stability.

Endnotes

[1] Melissa Dalton et al., *By Other Means Part II: Adapting to Compete in the Gray Zone* (Washington, DC: CSIS, August 2019), https://www.csis.org/analysis/other-means-part-ii-adapting-compete-gray-zone.

[2] All three distances are measured along the ground from the point directly beneath the HAPS to the location of the target. See: "Airbus Zephyr: Unique Contribution to Decision Superiority," Airbus Defence and Space, 2017, https://www.airbus.com/content/dam/corporate-topics/publications/brochures/0612_17_zephyr_datasheet_e_horizontal_a4_lowres.pdf.

[3] Pedro Valdez and Paulina Wheeler, "High Altitude Pseudosatellites," On the Radar, CSIS, July 29, 2019, https://ontheradar.csis.org/issue-briefs/high-altitude-pseudosatellites/.

[4] Iftikhar Ali et al., "Satellite Remote Sensing of Grasslands: From Observation to Management," *Journal of Plant Ecology* 9, no. 6 (2016): 649-71; Guijun Yang et al., "Unmanned Aerial Vehicle Remote Sensing for Field-Based Crop Phenotyping: Current Status and Perspectives," *Frontiers in Plant Science* 8 (2017): 1-26.; W. Carter Johnson et al., "Modeling Seed Dispersal and Forest Island Dynamics," in *Ecological Studies Forest Island Dynamics in Man-Dominated Landscapes*, R.L. Burgess and D.M. Sharpe, eds. (December 1981), 215-39; Jeremy H. Groves et al., "Modelling of Floating Seed Dispersal in a Fluvial Environment," *River Research and Applications*, 2009, no. 25 (2009): 582-92.

[5] Jake Hecla, "Light Detection and Ranging (LIDAR)," On the Radar, CSIS, July 29, 2019, https://ontheradar.csis.org/issue-briefs/light-detection-and-ranging-lidar/.

[6] "Echo Voyager," Boeing, https://www.boeing.com/defense/autonomous-systems/echo-voyager/index.page.

[7] H. I. Sutton, "China Navy Reveals New Large Underwater Robot Which Could Be A Game Changer," *Forbes*, October 1, 2019, https://www.forbes.com/sites/hisutton/2019/10/01/china-reveals-new-robot-underwater-vehicle-hsu-001/#31cd33c21991.

[8] Ben Werner, "Navy's Knifefish Unmanned Mine Hunter Passes Sea Acceptance Testing," USNI News, June 5, 2018, https://news.usni.org/2018/06/05/navys-knifefish-unmanned-mine-hunter-passes-key-test.

[9] Megan Eckstein, "Boeing, Lockheed Martin Moving Forward with Navy XLUUV Acquisition Program," USNI News, October 2017, https://news.usni.org/2017/10/17/28810.

[10] Nate Frierson and Lizamaria Arias, "Artificial Intelligence Analysis Applications," On the Radar, CSIS, July 29, 2019, https://ontheradar.csis.org/issue-briefs/artificial-intelligence-analysis-applications-a-technology-primer/.

[11] Natalie Sherman, "Is China Gaining an Edge in Artificial Intelligence?," BBC News, November 12, 2019, https://www.bbc.com/news/business-50255191.

[12] Phil Stewart, "Deep in the Pentagon, a Secret AI Program to Find Hidden Nuclear Missions," Reuters, June 5, 2018, https://www.reuters.com/article/us-usa-pentagon-missiles-ai-insight/deep-in-the-pentagon-a-secret-ai-program-to-find-hidden-nuclear-missiles-idUSKCN1J114J.

[13] Cheryl Pellerin, "Project Maven to Deploy Computer Algorithms to War Zone by Years End," DoD News, Defense Media Activity, July 21, 2017, https://dod.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/.

[14] Stewart, "Deep in the Pentagon."

[15] Lora Saalman, ed., *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk: East Asian Perspectives*, Vol. 2, (Stockholm, Sweden: Stockholm International Peace Research Institute, October 2019), https://www.sipri.org/publications/2019/other-publications/impact-artificial-intelligence-strategic-stability-and-nuclear-risk-volume-ii.

[16] Amy Butler and Bill Sweetman, "Secret New UAS Shows Stealth, Efficiency Advances," *Aviation Week & Space Technology*, December 6, 2013, http://aviationweek.com/defense/secret-new-uas-shows-stealth-efficiency-advances.

[17] Richard Tompkins. "BAE Systems developing new sonar for U.S. Navy submarines," UPI, July 18, 2017, https://www.upi.com/Defense-News/2017/07/18/BAE-Systems-developing-new-so-

nar-for-US-Navy-submarines/3081500391180/.

18 Frederic Bouchard et al., "High-dimensional quantum cloning and applications to quantum hacking," *Science Advances* 3, no. 2, (February 2017), doi:10.1126/sciadv.1601915.

19 It is important to note that different names do not necessarily denote separate entities. See "Lazarus Group," MITRE, ATT&CK, accessed February 19, 2020, https://attack.mitre.org/groups/G0032/; Nalani Fraser "APT38: Details on New North Korean Regime-Backed Threat Group," FireEye, October 3, 2018, https://www.fireeye.com/blog/threat-research/2018/10/apt38-details-on-new-north-korean-regime-backed-threat-group.html; "North Korean Malicious Cyber Activity," CISA, accessed February 19, 2020, https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity; https://securityaffairs.co/wordpress/67895/apt/north-korea-group-123.html; and Adam Meyers "Advanced Persistent Threat List: Types of Threat Actors," CrowdStrike, December 12, 2019, https://www.crowdstrike.com/blog/meet-the-adversaries/.

20 "North Korea's Ruling Elite Adapt Internet Behavior to Foreign Scrutiny," Recorded Future, April 25, 2018, https://www.recordedfuture.com/north-korea-Internet-behavior/.

21 Hecla, "Light Detection and Ranging (LIDAR).".

22 Lieber and Press, "The New Era of Counterforce.".

23 Wang Yi, "ADASpace set to star in AI satellite constellation sphere," *Global Times*, June 30, 2019, http://www.globaltimes.cn/content/1156263.shtml.

24 Valdez and Wheeler, "High Altitude Pseudosatellites."; See example: United Kingdom orders additional Zephyr," Airbus Defense and Space, August 18, 2016, https://www.airbus.com/newsroom/press-releases/en/2016/08/united-kingdom-orders-additional-zephyr.html.

25 "Beihang Successfully Researches and Develops Our Nation's First Chang Ying Large Long-Endurance UAV" [北航成功研制我国首款长鹰大型长航时无人机], Sina, September 13, 2011, http://mil.news.sina.com.cn/2011-09-13/1345665189.html; Chris Biggers, "Satellite Imagery Reveals China's New Drone Base," bellingcat, June 29, 2015, https://www.bellingcat.com/news/rest-of-world/2015/06/29/satellite-imagery-reveals-chinas-new-drone-base/?utm_source=Sailthru&utm_medium=email&utm_term=%2ASituation Report&utm_campaign=SitRep0630; Ankit Panda, "Meet China's East China Sea Drones," Diplomat, June 30, 2015, https://thediplomat.com/2015/06/meet-chinas-east-china-sea-drones/.

26 "RQ-4 Global Hawk Fact Sheet," United States Air Force, October 2014, https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104516/rq-4-global-hawk/.

27 Reddie and Goldblum, "Unmanned Underwater Vehicle (UUV) Systems for Submarine Detection."

28 Stephen Chen, "China military develops robotic submarines to launch a new era of sea power," *South China Morning Post*, July 22, 2018, https://www.scmp.com/news/china/society/article/2156361/china-developing-unmanned-ai-submarines-launch-new-era-sea-power.

29 McCormick, "United States Situational Awareness."

30 Department of Defense, "Department of Defense Announces Successful Micro-Drone Demonstration," Press Release, January 9, 2017, https://dod.defense.gov/News/News-Releases/News-Release-View/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration/.

31 Ibid.

32 Andrew Reddie and Bethany Goldblum, "Smallsats," On the Radar, CSIS, May 4, 2019, https://res.cloudinary.com/csisideaslab/image/upload/v1562865065/on-the-radar/Smallsats%20Final%20Primer%20Formatted%2007-02-29.pdf.

33 McCormick, "United States Situational Awareness."

34 U.S. Army Training and Doctrine Command, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: December 2018), https://info.publicintelligence.net/USArmy-MultidomainOps2028.pdf.

35 Elsa Kania, "China's Strategic Situational Awareness Capabilities," On the Radar, Center for

Strategic and International Studies, July 29, 2019, https://ontheradar.csis.org/issue-briefs/china-situational-awareness/.

36 Ibid.

37 Ibid.

38 From a forthcoming primer to be published on the On the Radar website by Jason Arterburn.