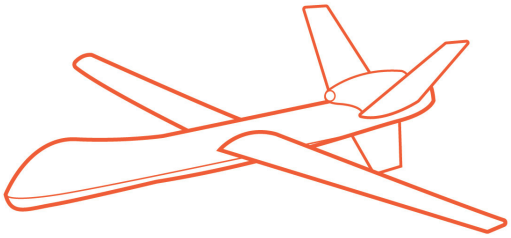


3 | Risk Factors of Situational Awareness Technology and Strategic Stability

Advanced Strategic SA Capabilities and Stability Risks

Strategic stability generally depends upon the combination of the absence of incentives to use nuclear weapons first (crisis stability) and the absence of incentives to build up a nuclear force (arms race stability).[1] Schelling was the first to posit that crisis stability occurs "if neither side has or perceives an incentive to use nuclear weapons first out of the fear that the other side is about to do so."[2] Arms race stability, on the other hand, generally refers to a situation in which neither side has the incentive to augment their forces—qualitatively or quantitatively—based on the fear that their opponent could gain a meaningful advantage.[3] While strategic stability depends upon factors including successful crisis management, decreasing incentives to use nuclear weapons, and reducing incentives for longer-term arms races, this study focuses broadly on the escalatory pressures in crisis that could be influenced positively or negatively by the emerging strategic SA ecosystem- including those pressure points that could appear well below the nuclear threshold.

All the strategic SA capabilities considered in this study can, to some degree, introduce risks for strategic stability. These risks can be characterized as: intrusive, destructive, predictive, preemptive, dual-use, clandestine, vulnerable, and action-enabling. Like the attributes in the previous chapter, some risk factors are more common than others: for example, many technologies may be considered "action-enabling," as they enable military options that were previously difficult to achieve. The study team developed and used a set of stability risk factors to evaluate the extent and manner in which escalatory risk—either in terms of creating incentives for escalatory military action that might prove uncontrollable or increase the likelihood of miscalculation with escalatory outcomes—could be associated with emerging SA capabilities. These risk factors are elaborated upon in Figure 3.1. This common set of criteria allowed for more consistent comparisons across the range of different technologies in terms of evaluating their risk potential. Figure 3.1 defines each of these escalatory risk factors and provide illustrative examples.

Figure 3.1: Risk Factors Associated with Emerging SA Technologies

RISK FACTORS		
STABILITY RISK FACTOR	**DEFINITION**	**TECHNOLOGY EXAMPLES**
Predictive	*The degree to which a capability allows a state to anticipate adversary actions as opposed to merely reacting to them after they are completed.*	*AI decision support tools that examine patterns of behavior and detect anomalies to improve the accuracy and timeliness of warning.*
Preemptive	*The extent to which a capability enables acting against adversary actions or plans before they can be completed.*	*Air, ground, or sea-based sensors that can detect the movement of mobile missiles prior to launch.*
Action-enabling	*The degree to which a capability enables new military options.*	*Cyber exploit that can identify and (if desired) disable network or space-based capabilities; or unmanned air or maritime surveillance capabilities that can identify and locate adversary capabilities and provide real-time targeting.*
Intrusive	*The extent to which a capability must enter an adversary's territory, airspace, or networks.*	*An autonomous UUV or UAV with advanced sensing capability deployed inside adversary territory, airspace, or waters.*
Destructive	*The extent to which a capability can disable or degrade an adversary system, either temporarily or permanently, in achieving its objective.*	*A cyber exploit that can detect a decision message by an adversary and disrupt or alter the message at the same time.*
Clandestine	*The extent to which capabilities derive significant military advantage by being kept secret and pose significant disadvantage if revealed.*	*Use of covert personnel or capabilities to deploy highly advanced sensing capabilities in adversary territory.*
Vulnerable	*The degree to which an adversary can deny the use of a capability.*	*Air, maritime, or space surveillance assets that are vulnerable to shoot down, spoofing, or blinding.*
Dual-use	*The extent to which a capability is used for conventional and nuclear missions.*	*Space-based surveillance or communications systems that support both conventional and nuclear missions.*

Assessing Risk in the Emerging Strategic SA Ecosystem

PREDICTIVE, PREEMPTIVE, AND ACTION-ENABLING

Predictive, preemptive, and action-enabling capabilities are similar in that their escalatory risks are associated with the collection of certain information that could incentivize military actions through a perceived offensive advantage. Such actions are wide ranging but could include the collection of information that enables or encourages offensive first-mover actions (such as precision targeting of dual-use delivery systems) or defensive actions that could be perceived as escalatory if detected by the other side (such as dispersing nuclear weapons to improve survivability in a damage-limitation strategy). While all three risk factors are closely related, emphasizing their differences is important for understanding how they may independently impact strategic stability.

PREDICTIVE

Predictive risk factors describe the degree to which a capability allows a state to anticipate adversary actions in advance as opposed to merely reacting to them after they are initiated. Predictive technologies could potentially provide insight into the movement of adversary forces, the deployment of weapons systems, or even adversary intent to initiate military conflict before such actions would otherwise be perceived by traditional strategic SA capabilities (e.g., early-warning satellites designed to detect missile launches post-launch). Even if a predictive capability does not provide specific targeting information, it may prompt decisionmakers to act in an anticipatory fashion, diplomatically or militarily. On the other hand, when faced with predictive capabilities, the targeted country may feel increased "use or lose" pressures that could lead to escalatory outcomes. Decisionmakers could also use information collected by predictive capabilities to further enhance their strategic SA in concert with other capabilities. For example, if a predictive technology detected that an adversary is likely to take an action (e.g., fueling missiles in preparation for launch), decisionmakers could employ other capabilities to surveil the area and improve certainty (e.g., focusing satellite sensors on launch pads to verify missile launch preparations).

Even if a predictive capability does not provide specific targeting information, it may prompt decisionmakers to act in an anticipatory fashion, diplomatically or militarily.

The predictive nature of AI technologies is representative of the challenges associated with such capabilities. For example, predictive analytics applications could ingest large amounts of data and discover previously unknown but strategically relevant anomalies, enabling more accurate and timely information for analysts.[4] While obviously advantageous for the state employing such a capability, the predictiveness of such a system could pose stability risks. Analysts using such an application could potentially predict the mobilization of forces or planning for a snap invasion by a competitor, incentivizing a military response before the window of opportunity closes. .[5]

PREEMPTIVE

Preemptive capabilities not only anticipate adversary action, but also enable disruptive responses to adversary actions or plans before they can be completed. While similar to predictive risk, preemptive capabilities can exist independently from one another. For example, while AI analysis applications may provide predictive insight into adversary actions, such a capability would not be preemptive if it does not provide incentive and opportunity to counter the action before it is completed.

On the other hand, a UAV deployed to monitor an adversary's mobile missiles would be a preemptive capability if it were able to detect mobile nuclear missiles moving out of garrison and enable actions to disrupt the missile deployment, such as destroying the missiles themselves or destroying the road to limit their movement.

Preemptive actions could also be defensive in nature but may be viewed as offensive and escalatory by the adversary, given the nature of security dilemma dynamics.[6] One example of this risk factor would be moving one's own nuclear weapons to maintain second-strike capability in response to information that an adversary is surveilling such assets. While such an action is defensive as it relates to protecting one's own forces, it would in effect be preempting an adversary's (potential)

actions against said forces, which could in turn incentivize the adversary to strike before the weapons have been moved, thus risk upending strategic stability.

ACTION-ENABLING

The final risk factor most closely associated with predictive and preemptive capabilities is "action-enabling," or the degree to which a capability enables new military options. This risk factor is perhaps the most intuitively destabilizing, as military options can risk escalating a crisis into a full-blown conflict or escalate a conflict from the conventional to the nuclear level. A capability that is either predictive or preemptive may enable further information collection or simply provide insight into an adversary's forces, whereas action-enabling capabilities inherently enable military options.

Spoofing is an example of an action-enabling capability that could create escalatory pressures during crisis or conflict. Spoofing (a form of electronic attack where the attacker tricks a receiver into believing a fake signal, produced by the attacker, is a genuine signal) could be used to take control of a satellite by successfully spoofing the command and control uplink signal.[7] If the satellite being spoofed is used for both conventional and nuclear missions and the adversary is unable to discern the intent of the attack, it may raise the perceived stakes in a crisis and lead to escalation.

INTRUSIVE

The intrusive risk factor describes the extent to which a capability must enter an adversary's territory (land or maritime), airspace, or networks to accomplish its task. This action may be viewed as a risk to strategic stability. Intrusive capabilities often violate traditional concepts of territorial sovereignty and provide opportunities for misperception of intent. Examples of intrusive capabilities include UAVs that violate adversary airspace, UUVs that loiter near adversary submarine bases, or the placement of compact, multisensor proximity devices near land targets (potentially placed by SOF inserted into adversary territory).

In addition to these examples of intrusive capabilities in the traditional sense (violating territorial sovereignty), cyber surveillance capabilities can also be considered intrusive, as they violate private networks that transmit sensitive communications. This poses risks to strategic stability, as the collected information can concern either conventional or nuclear forces and the targeted state may be unable to discern what type of specific information is being collected. If decisionmakers believed their NC3 was being electronically monitored, this could lead to escalation in crisis scenarios.

DESTRUCTIVE

Destructive risk factors describe the extent to which a capability can disable or degrade an adversary system, either temporarily or permanently, in pursuit of its information gathering objective. This risk factor is uncommon in the strategic SA capabilities explored in this project, as such capabilities are primarily concerned with collecting information rather than degrading adversary capabilities, but some strategic SA capabilities can be destructive in the course of their information collection. For example, a cyber surveillance exploit that can monitor adversary communications could also be destructive if it were able to alter, disrupt, or delete messages between high-level government and military leaders. Such actions may endanger strategic stability if an adversary perceived that electronic tampering was intended to disrupt communications with their nuclear forces, hinder the execution of nuclear operations, or stall reactions to an imminent nuclear strike.

Defense and countering strategic SA capabilities are also inherently destructive to some degree, as they seek to degrade adversary systems or defend against threats and thus neutralize attacks. Satellite jamming is an example of a destructive strategic SA capability in which an electronic anti-satellite (ASAT) attack interferes with radio frequency communications by generating noise in the same frequency band and within the field of view of the antenna on the targeted satellite or receiver. While not as destructive as kinetic ASAT weapons, satellite jamming can disrupt adversary communications and degrade their ability to function, which could cause escalation during a crisis scenario. This dynamic could threaten strategic stability, especially if the satellites targeted by jamming are dual use (used for conventional and nuclear missions) and adversaries are unable to discern intent (see section on entanglement, Chapter 4.2)

CLANDESTINE

If a capability is clandestine, it derives significant military advantage from being kept secret but also can pose significant disadvantage and risk if revealed.[8] DOD doctrine defines clandestine activities as "operations sponsored or conducted by governmental departments in such a way as to assure secrecy or concealment" that may include relatively "passive" collection and information gathering operations.[9] If a technology is clandestine, it means that it is "hidden," where the aim is for it to not be noticed at all. In contrast, covert means "deniable," such that if the technology is noticed, it is not attributed to a group.[10] For example, plant-based sensors can be classified as clandestine, as they could be deployed on adversary territory; an adversary aware of deployed plant-based sensors would remove them, block their ability to report, block their ability to detect, or avoid the limited range of detection these plant-based sensors would have. However, successfully deployed modified plants would be very hard to identify in an environment, and their existence may be unknown. Adversaries who discover plant-based sensors in their territory may not be able to immediately identify who deployed the smart plants as the biological material would not necessarily have any perceptible human or technological trace.[11]

VULNERABLE

In addition, vulnerability of SA technologies—defined as the degree to which an adversary can deny the use of a capability—is another risk to strategic stability. Technological vulnerability—the chance of failure of an entire technological system due to outside events—is in stark contrast to when a technological system can be said to be resilient (i.e., if it can maintain its purposes in the face of a threat).[12] Adversaries are likely to disrupt or destroy strategic SA capabilities that are more vulnerable, thereby cutting off the flow of information. For instance, emerging technologies for SA in the air, maritime, or space domain could potentially be vulnerable to shootdown, spoofing, or blinding.

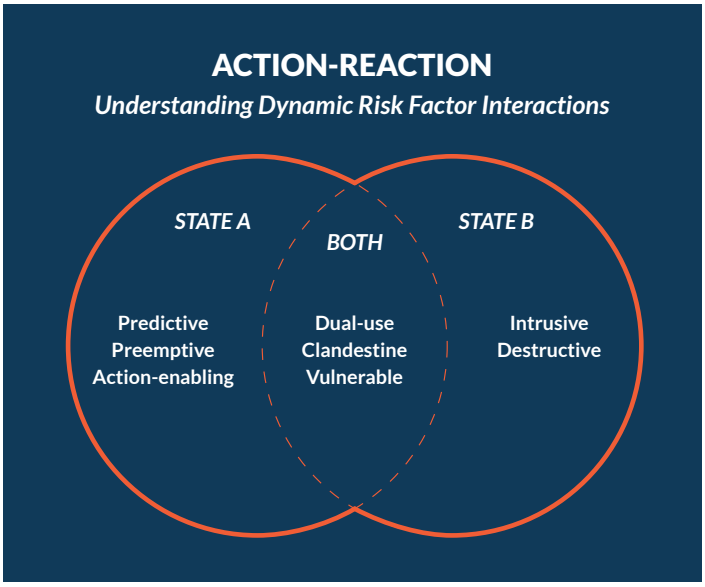
DUAL-USE

Dual-use capabilities are those that are used for both conventional and nuclear surveillance or warning missions. The dual-use nature of emerging technologies can create confusion as to the intentions of the surveilling party. For example, if UUVs are used to observe an adversary's conventional submarines (SSNs), which might be housed alongside its nuclear-armed ballistic missile submarines (SSBNs), the surveilled state would be unable to tell which assets were being targeted and may deem their nuclear assets as under threat. Dual-use capabilities may further upset strategic stability vis-à-vis the escalation pathway of entanglement (explored in Chapter 4).

Action-Reaction: Understanding Dynamic Risk Factor Interactions

As shown in Figure 3.2, escalation plays out dynamically between two or more actors in a crisis, each managing their own perception of risk and reacting to the actions of the other. The risk factors described above can interact in unique and complex ways as actors weigh the costs and benefits of using capabilities to increase their strategic SA relative to an adversary. In some cases, these risks manifest as a perception that escalation can be managed on reasonably favorable terms; in other cases, they manifest as a misunderstanding of the other actors' intentions. The following Venn diagram suggests how the pursuit of information dominance by a hypothetical "State A" employing a strategic SA capability may create both first-mover and miscalculation risks relative to the target, "State B."

Figure 3.2: Action-Reaction Dynamics among Risk Factors



This dynamic can be illustrated with an example scenario, such as the deployment of a HALE UAV over adversary territory. In this example, State A introduces an intrusive risk to which State B may feel compelled to respond to militarily, either because it perceives the violation of its territory as an act of war itself or because it believes the surveillance is a precursor for attack by State A. The UAV deployment, if successful, can introduce a preemptive or action-enabling risk by producing information that incentivizes State A to escalate militarily in hopes of capturing a strategic advantage or terminating the conflict before State B is able to take further action. Such first-mover incentives may be viewed by State A as controllable or conventional, at least initially, which may contribute to their appeal. On the other hand, the HALE UAV is vulnerable, since it is detectable and easily targeted with advance air defense assets. If it is targeted by State B and shot down, State A chooses whether to accept the loss or escalate—in essence, drawn into further conflict by an intrusive and vulnerable asset.

Another example, such as a cyber exploit used to surveil adversary networks, could pose risks of misperception for both states involved. In this hypothetical scenario, State A employs an intrusive and potentially destructive exploit into State B's networks. The information gained may be preemptive or even predictive if AI programs are used to analyze the large amounts of data collected. State A may view the exploit as maintaining a "baseline" of surveillance given the constant back and forth common in cyber competition today, but should the clandestine surveillance be detected, State B may question the intent of such surveillance (especially if the network is dual use and used in both conventional and nuclear missions). This scenario is plausible given publicly available military doctrine. For example, the 2018 DOD Cyber Strategy

This interplay of risk factors can contribute to our understanding of how the pursuit of information dominance may contribute to escalation, either by incentivizing first-mover actions or by heightening miscalculation risks during crises between nuclear-armed adversaries.

outlines an official "defend forward" doctrine that aims to "disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[13] This poses risks to strategic stability, as the probing may be intended for defensive measures (collecting information about cyber threats to stop them before they can be employed against U.S. targets), but the targeted state may perceive the action as a threat to either conventional or nuclear missions, particularly during a crisis.

This interplay of risk factors can contribute to our understanding of how the pursuit of information dominance may contribute to escalation, either by incentivizing first-mover actions or by heightening miscalculation risks during crises between nuclear-armed adversaries.

Risk Versus Reward: Evaluating Strategic SA Capabilities

The study team examined 28 different technical capabilities with application to strategic situational awareness in terms of both their key attributes and their potential stability risks. These technical capabilities were presented during tabletop exercises. Figure 3.3 outlines the technologies explored by this project. The table is not exhaustive, but it represents strategic SA capabilities across all domains and is representative of the emerging SA ecosystem.

Which Technologies Were Explored During On the Radar?

SEA AIR LAND
SPACE CYBER DEFENSE/COUNTERING

P = PLATFORM
CE = CRITICAL ENABLER

STRATEGIC SA CAPABILITY	DOMAIN & TYPE	DEFINITION	EXAMPLE OF STRATEGIC SA APPLICATION	DEMONSTRATIVE TECHNOLOGY	DOMINANT ATTRIBUTES	DOMINANT RISK FACTORS
Autonomous Unmanned Underwater Vehicle (UUV)	P	Sea-based sensor platform with little to no human input	Employed to track submarine and surface vessels	Large Diameter UUV (LDUUV)	Vantage/ Range, Persistence	Intrusive, Preemptive
Unmanned Underwater Vehicle (UUV) Swarms	P	Groups of UUVs networked together	Swarms to specific submarine or surface vessel target (including ports)	Aquabotix UUV Swarm	Persistence, Resiliency/ Reliability	Intrusive, Action-enabling
Unmanned Underwater Vehicle (UUV) Nets	P	UUVs deployed to passively monitor geographic chokepoints	Static/slow-moving UUVs deployed to littoral waters/geographical chokepoints to track submarineand surface vessel activity		Persistence, Precision	Preemptive, Clandestine
Unmanned Surface Vehicle (USV)	P	Unmanned surface platform capable of being underway for weeks on end	Used to patrol, track, and deploy a range of smaller USV and UUV systems	U.S. Navy Autonomous Swarmboats; Aquabotix USV Swarm	Vantage/ Range, Precision	Intrusive, Vulnerable
High Altitude Long Endurance (HALE) UAV	P	Unmanned aerial vehicle with wide range of sensor capabilities	Surveil adversary capabilities at high-altitude and maneuverable to lower altitudes	RQ-4, RQ-180	Vantage/ Range, Precision	Intrusive, Vulnerable
High Altitude Pseudosatelites	P	Extremely high-altitude UAVs with length-ened wingspan able to surveil an area of interest for days to weeks	Provides long-term, persistent coverage of land and surface targets from over 65k feet in altitude	Airbus Zephyr; Boeing PhantomEye	Vantage/ Range, Persistence	Intrusive, Vulnerable
Unmanned Aerial Vehicle (UAV) Swarms	P	Groups of UAVs networked together to surveil targets in close proximity	Deployed to surveil land and sea targets at short distance	DARPA Gremlins Program	Vantage/ Range, Resiliency/ Reliability	Intrusive, Action-enabling
Unmanned Underwater Vehicle (UUV)-Launched Unmanned Aerial Vehicle (UAV)	P	Small UAV deployed from UUV with limited optical sensors and comms capabilities	Designed to take aerial images of coastal targets in close proximity		Speed, Precision	Intrusive, Preemptive
Autonomous Unmanned Aerial Vehicle (UAV)	P	Next-generation unmanned aircraft with both reconnaissance and warfighting capabilities	Provides aerial imaging and real-time reconnais-sance over land and sea targets	Predator MQ-1, MQ-9, MQ-X	Vantage/ Range, Precision	Intrusive, Vulnerable, Dual-use
Manned, Next-Gen Stealth Aircraft	P	Next-generation manned stealth aircraft equipped with optical sensors	Performs high-altitude reconnaissance missions of and and sea targets	Lockheed TR-X	Speed, (Un)detectability	Intrusive, Dual-use
Smallsat Constellations	P	Small satellites networked together to surveil target	Employs advanced sensors from space to surveil targets	SensorSat	Persistence, Resiliency/ Reliability	Preemptive, Dual-use
Co-Orbital Reconnaissance Satellites	P	Small satellites placed in a similar orbit to their target	Tracks and monitors space-based adversary capabilities including satellites used for surveillance, communications, and early warning		Vantage/ Range, Persistence	Dual-use, Clandestine
Quantum Computing	P	Computers that take advantage of physics at the quantum level	Enables increasingly rapid data analysis as well as processing power for increasingly autono-mous systems	China's National Laboratory for Quantum Information Science	Speed, (Un)detectability	Predictive, Action-enabling
Artificial Intelligence (AI) Analysis applications	CE	Computer applications to support human analysts and decision-makers	Reconciles diverse data streams to rapidly provide pattern recognition and anomaly detection tools to analysts	Project Maven	Speed, Precision	Predictive, Vulnerable
Cyber Surveillance	CE	Software and hardware that provides access to an adversary's computer network	Provides insight into adversary behavior, intentions, and decision-making	Eternal Synergy and Double Pulsar	(Un)detectability, Persistence	Intrusive, Clandestine

Which Technologies Were Explored During On the Radar

(continued)

SEA AIR LAND SPACE CYBER DEFENSE/COUNTERING

P = PLATFORM

CE = CRITICAL ENABLER

STRATEGIC SA CAPABILITY	DOMAIN & TYPE	DEFINITION	EXAMPLE OF STRATEGIC SA APPLICATION	DEMONSTRATIVE TECHNOLOGY	DOMINANT ATTRIBUTES	DOMINANT RISK FACTORS
Compact, Multisensor Proximity Devices	CE	Credit-card sized secure, low-resolution wireless sensors	Passive sensors placed close to land target location. Example target includes nuclear fuel fabrication facilities		Precision, Persistence	Intrusive, Clandestine
Plant-based Sensors	CE	Physiology-based sensors capable of reporting the presence of various stimuli	Employed in adversary territory to monitor for certain chemical or radiological signatures associated with activities of interest	DARPA Advanced Plant Technologies Program	Vantage/ Range, (Un)detectability	Intrusive, Clandestine
Light Detection and Ranging (LIDAR)	CE	A sensor that generates spatial data from light reflected from a laser	Rapidly 3D maps a target area from air, space, or the surface of the ocean with potential tracking capabilities	DARPA HALOE	Precision, Persistence	Dual-use, Preemptive
Hyperspectral Sensors	CE	Takes hundreds or thousands of contiguous images in narrow wavebands	Provides a picture of adversary behavior using hyperspectral images that cut through obstacles to optical sensors	ACES-Hy UAV sensor	Vantage/ Range, Precision	Dual-use, Preemptive
Non-acoustic Submarine Detection	CE	Detection technologies including light-based imaging and magnetic detection	Magnetometers, in particular, are used to attempt to track adversary submarines	China's Guanlon Project	Vantage/ Range, Precision	Clandestine, Action-enabling
Remote Radiation Detection by Electromagnetic Air Breakdown	CE	Uses the reflection of high-intensity pulses to probe the concentration of charged species produced by ionization in air	Used to detect nuclear activity in facilities across the fuel cycle.		Vantage/ Range, Precision	Intrusive, Preemptive
Electro-Optical (EO) Sensor	CE	Use lenses and mirrors to image objects across the electromagnetic spectrum	Used to detect and track aircraft, missile launch warning, target acquisition and surveillance, etc.	ARGUS	Vantage/ Range, Precision	Dual-use, Preemptive
Gravity Gradiometer	CE	Passive sensor that measures minute differences in the earth's density	Yields information on geologic structures underground and undersea used to surveil tunneling by adversaries		Vantage/ Range, Precision	Dual-use, Preemptive
Synthetic Aperture Radar (SAR)	CE	Radar-based sensor used to build high-resolution imagery from mobile platforms	Used to surveil and detect land-based assets such as mobile missiles	RADARSAT-2	Precision	Dual-use, Preemptive
Inverse Synthetic Aperture Radar (ISAR)	CE	Uses movement of the target to generate high-resolution images	Able to image moving objects from a variety of vantage points		Precision	Dual-use, Preemptive
Cognitive Electronic warfare		Uses AI to enhance development and operation of electronic warfare technologies	Used in attempt to detect, suppress, and neutralize cyber attacks		Speed, Persistence	Predictive, Clandestine, Destructive
Spoofing		Cyber attack in which attacker masquerades as legitimate user and provides false data to the system	Can be used to take control of a satellite or inject corrupt data into communications or otherwise poison data from SA sources		Vantage/ Range, Precision	Intrusive, Action-enabling, Destructive
Satellite jamming		Electronic anti-satellite (ASAT) attack that interferes with communications traveling to and from a satellite (downlink and uplink)	Can be used to disrupt missile warning systems, SIGINT, GPS, and communications satellites	Krasukha-2, Zhitel, and Borisglobesk	Persistence, Resiliency/ Reliability	Action-enabling, Destructive

Endnotes

1 James M. Acton, "Reclaiming Strategic Stability," in *Strategic Stability: Contending Interpretations*, Elbridge A. Colby and Michael S. Gerson, eds., (Carlisle Barracks, PA: Strategic Studies Institute, 2014), 117–146.

2 Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1980).

3 Acton, "Reclaiming Strategic Stability."

4 Paul Scharre and Michael C. Horowitz, *Artificial Intelligence: What Every Policymaker Needs to Know* (Washington, DC: Center for a New American Security, 2018), https://www.cnas.org/publications/reports/artificial-intelligence-what-every-policymaker-needs-to-know. .

5 Ibid.

6 Robert Jervis, "Cooperation Under the Security Dilemma," World Politics 30, no. 2 (1978): 167-214, accessed February 10, 2020, www.jstor.org/stable/2009958.

7 Todd Harrison, Kaitlyn Johnson, and Thomas G. Roberts, *Space Threat Assessment 2019* (Washington, DC: CSIS, April 2019), https://www.csis.org/analysis/space-threat-assessment-2019.

8 Austin Long and Brendan Rittenhouse Green, "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy," *Journal of Strategic Studies* 38, no. 1-2 (2015): 38-73, https://www.tandfonline.com/doi/pdf/10.1080/01402390.2014.958150.

9 Michael E. Devine, "Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions in Brief," Congressional Research Service, June 14,2019, https://fas.org/sgp/crs/intel/R45175.pdf

10 Ibid.

11 Benjamin, "Plant-based Sensors."

12 Brian Martin, "Technological Vulnerability," *Technology in Society* 12, no. 4 (1996): 511-523, https://documents.uow.edu.au/~bmartin/pubs/96tis.html.

13 "Summary: Department of Defense Cyber Strategy 2018," DOD, September 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.