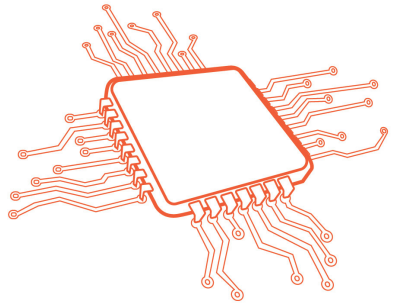


# 4 | Pathways to Escalation

Of particular concern are three potential escalation pathways—provocation, entanglement, and information complexity—that may be triggered or exacerbated by the use of emerging strategic SA-enhancing capabilities. Although multiple pathways may be activated during an actual crisis, either simultaneously or sequentially, examining each of these escalatory pathways individually provides insight into the interplay of strategic SA technologies and stability risks.

## *Provocation*

The active nature of the emerging strategic SA ecosystem means that states have the capability to penetrate adversary territory (via land, sea, and air) and networks to gain increasingly precise and potentially actionable information. However, the use of these capabilities risks discovery and response by the state under surveillance. Likewise, these capabilities may generate information that suggests the opening of an offensive window of opportunity, greatly increasing incentives to move first. Escalation through provocation occurs when parties to a crisis lack an ability to determine the offensive or defensive intentions behind a proposed action or information collection effort, greatly intensifying escalatory pressures. It may occur because:

- information collection efforts begin to influence rather than observe the course of a conflict or crisis (whether intentional or not) through intrusive or disruptive activity; or
- the rapid, precise, and persistent nature of SA capabilities creates opportunities or incentives to take action on a preemptive or preventive basis.

In other words, a provocation-based escalation cycle occurs when the use of these technologies is perceived in offensive terms by the country being observed (e.g., by illegal territorial intrusion) or the strategic SA capabilities afford a significant offensive or first-mover advantage to the observing state.

These provocation dynamics could play out through several different scenarios:

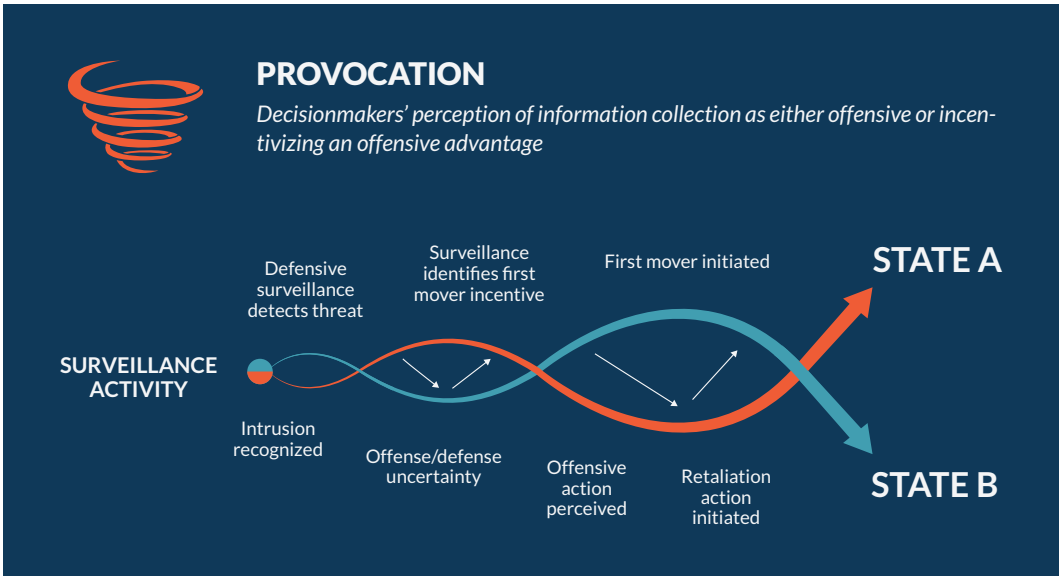
1. The use of intrusive technologies challenges legal and political concepts of sovereignty and is perceived as offensively intended (a territorial incursion can be perceived as an act of war regardless of its defensive intent);
2. The intended mission of these capabilities (general surveillance versus counterforce support or surveillance versus strike) is not readily identifiable and is misperceived;

3. Surveillance capabilities intentionally or unintentionally approach vital strategic assets as they conduct surveillance and therefore provoke a response;

4. Clandestine capabilities, such as active cyber surveillance, are discovered, prompting surprise and uncertainty as to risks and damage; and

5. Surveillance capabilities initiated for defensive purposes identify preemptive or action-enabling options, prompting a willingness to take an escalatory offensive action in hopes of terminating the crisis on favorable terms. Or, if the surveillance is detected or revealed, the country under surveillance may assume such intentions and undertake an escalatory step of its own.

Figure 3.2: Action-Reaction Dynamics among Risk Factors




## OBSERVING VERSUS SHAPING

The very act of collecting information could provoke an escalatory response because many emerging systems are intrusive and may operate in ways that are perceived to violate state sovereignty. This may occur from the violation of internationally recognized or unilaterally proclaimed borders, territorial waters, and sovereign airspace but could also provoke a response by intruding in the far less well-defined and legally delineated domains of cyber and space.

If clandestine information gathering assets—such as cyber intrusions or unmanned systems believed to be stealthy—are discovered by an adversary operating within its territory, they could be indistinguishable from a destructive or offensive attack and be considered provocative. There

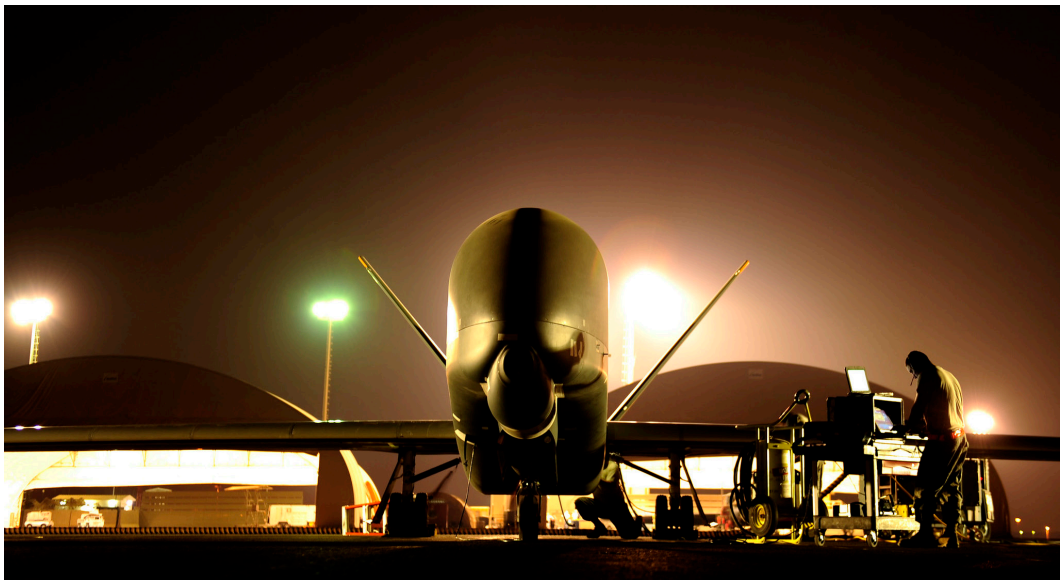
*The very act of collecting information could provoke an escalatory response because many emerging systems are intrusive and may operate in ways that are perceived to violate state sovereignty.*

is reason to believe assets used solely for information collection could nonetheless appear threatening to an adversary and provoke the use of force. As Robert Jervis and Mira Rapp-Hooper have written, "there is an all-too-human tendency to assume that an action will be seen as it is intended to be seen."[1] Nonetheless, as John Mearsheimer has recognized, "uncertainty about the intentions of other states is unavoidable," and "states can never be sure that other states do not have offensive intentions."[2] Inherent in the logic of a security dilemma is that states tend to view their own measures as defensive while interpreting those of other states as threatening.[3] In addition to intentions, states can also misperceive capabilities.[4] It seems likely that states would be susceptible to mischaracterize the purpose of SA assets as well, especially if they operate close to vital strategic assets as they conduct surveillance.

The role of unmanned systems in complicating perceptions of risk and provocation deserves particular attention, in part because of their increasing use. For the surveilling country, the use of unmanned assets might prove appealing due to the lack of risk to human life and lower perceived consequences of a loss. However, the surveilled country may perceive lower risks associated with attacking or disabling intrusive unmanned platforms and thus initiating an escalatory response. Also, technological developments that reduce the vulnerability of systems might both encourage intrusive uses and potentially make it difficult for adversaries to distinguish them from armed or offensive platforms, especially if surprised or spooked by the discovery of the intrusive or clandestine capability. For example, UAV platforms with low-observability characteristics might be employed in denied airspace, particularly in contexts in which an adversary has limited tools to detect an intrusion. UAVs are already used extensively for both SA and kinetic purposes, with few visible distinctions between armed and unarmed systems.[5] The use of surveillance drones has become so ubiquitous across conventional crisis and conflict, including counterterrorism operations, that decisionmaking procedures may lack guidance regarding their use under a nuclear shadow.

History provides some indication of how these escalatory dynamics may play out with unmanned systems. Pakistan has publicly denounced U.S. UAV missions in its airspace, objecting to any violation of state sovereignty.[6] In June 2019, Iran shot down an unmanned U.S. Navy RQ-4 Global Hawk surveillance aircraft, claiming it had been operating over its airspace—a claim disputed by U.S. officials.[7] This reportedly prompted planning by the United States for strikes against Iranian military facilities—an effort that was apparently called off at the last minute by the president.[8] Unmanned naval and subsurface systems, which could be used for intrusive operations in adversarial territorial waters or in contested areas, pose similar provocational challenges.

The cyber realm is another area particularly vulnerable to the provocation pathway, in large part because it can be especially challenging to delineate between offensive and defensive intentions in the cyber domain. The line between surveillance and attack is very thin, as techniques that would be useful to launch cyber probes mirror those of an offensive attack. Cyberattacks are often latent, and operations that are intended solely for espionage can sometimes transition to offensive purposes by adding onto the initial intrusion with malware modules.[9] Moreover, because cyberattacks may have unpredictable effects and are particularly prone to misestimations of "what the other side



*U.S. Air Force maintenance technicians conduct preflight checks on an RQ-4 Global Hawk unmanned aerial vehicle assigned to the 380th Expeditionary Operations Group at an undisclosed location in Southwest Asia Nov. 23, 2010.*

DoD photo by Staff Sgt. Andy M. Kin, U.S. Air Force/Released

thought it was doing," there is significant potential for misunderstanding and miscalculation.[10] The repercussions of this during peacetime might be limited, but during a crisis between nuclear-armed powers, there are risks that cyber surveillance targets could perceive an intrusion into their networks as a precursor to an attack. Compounding these potential misperceptions is the fact that there does not appear to be clearly defined differences between offense and defense across the cyber strategies of different countries.[11] The traditional nature of offense and defense in cyberspace is often different from that of the kinetic domains, and the intentions behind specific cyber operations—whether to protect one's own information or obtain access to another's—may be divorced from the tactics themselves.[12] Indeed, across the techniques of many cyber operations, the basic difference between surveillance and attack is "essentially a difference in intent."[13] Thus, what one party sees as cyber surveillance could appear highly aggressive and provoke escalation.

*The cyber realm is another area particularly vulnerable to the provocation pathway, in large part because it can be especially challenging to delineate between offensive and defensive intentions in the cyber domain.*

Of course, the capability to monitor activities associated with nuclear weapons could also prove highly stabilizing as a means of confirming assurances of non-aggressive intent, providing verifiable transparency and reducing risks of surprise while creating space for diplomacy and other tools to assist in de-escalating the crisis. That would require careful thinking about the relative value of covert versus overt techniques and the diplomacy and messaging associated with the use of potentially provocative surveillance capabilities.

## INCENTIVES AND OPPORTUNITIES FOR PREEMPTIVE OR PREVENTIVE ACTION

As conventional SA capabilities become more useful for nuclear warning, tracking, and targeting missions, both their utility to the surveilling country and perceived risk to the surveilled country grows.[14] While transparency of strategic-level capabilities has a stabilizing effect among great powers with credible second-strike survivability (and thus, mutually assured destruction), in dyads with significant nuclear asymmetry, greater knowledge of the location of the smaller country's strategic assets could undermine stability by shifting incentives for both countries toward using nuclear weapons first.[15] As Thomas Schelling observed, "the reciprocal fear of surprise attack" could destabilize a crisis and produce a war undesired by both parties.[16] Indeed, in crisis scenarios involving both conventional and nuclear weapons, game theoretic modeling suggests that developments that improve the capabilities of conventional forces to target nuclear assets are inherently destabilizing.[17]

Existing HALE UAV assets, for example, were originally intended for contingency and conventional wartime operations. However, they could also be useful to track a small country's nuclear mobile missiles or surveil for other warning indicators, such as the movements from garrison, changes in pattern of life, or the generation of forces. Constellations of small satellites could also offer the capability for real-time, continuous, high-definition visual and infrared imaging of areas of interest.[18] In conjunction with airpower, cruise missiles, and other conventional strike assets, such high fidelity surveillance capabilities may provide operators formidable capabilities for locating and engaging a range of targets.[19] Improved precision and coverage of surveillance technology is eroding the security that mobility once provided to survivability.[20] More broadly, U.S. intelligence capabilities for eroding second-strike forces are very advanced, according to some estimates, creating vulnerability for its second- and third-tier nuclear adversaries.[21]

For the targeted state, the ability of adversary strategic SA capabilities to inform or enable preemptive or preventive action may make it increasingly challenging to effectively conceal nuclear forces.[22] In such cases, the actual or perceived ability of the more technologically advanced country to carry out precision-strike missions against strategic nuclear assets will make any SA-enhancing activities—even those purely defensive in nature—seem highly provocative or escalatory. For example, if North Korea knew or suspected that the United States had the capability to track and destroy its nuclear mobile missiles, it might assume that any U.S. intelligence, surveillance, and reconnaissance assets in its airspace were a threat to its nuclear assets regardless of their actual assigned mission. Thus, highly intrusive surveillance assets could provoke escalation by creating pressure for the smaller nuclear power to "use or lose" its nuclear weapons and "posture its forces for an early use in a crisis, before its nuclear option is curtailed."[23]

For the technologically advanced country, the advancing precision of its surveillance and targeting capabilities could drive escalation in a crisis by increasing counterforce incentives of a "splendid" first strike that could disarm an adversary of its nuclear weapons before it could launch them in retaliation. By creating greater vulnerability for the targeted state's nuclear and missile forces, the targeting state may be more confident that a disarming escalatory strike would be successful and limit the possibility for retaliation.[24] Once capabilities such as UAVs identify possible targets, other conventional capabilities (often with higher-resolution sensors) are then able to continue the mission of precisely locating, identifying, and potentially targeting for kinetic action. Whereas UAVs can be denied access to adversary airspace, satellites orbit far above adversary territory and are much harder to disrupt (but still possible, depending on technical capabilities). An increasingly valuable capability for targeting both conventional and nuclear mobile assets is synthetic aperture radar (SAR). Until

recently, this type of radar employed on most satellites could not image moving targets, but over the past two decades, advances in data-processing techniques have enabled SAR to both detect moving targets and determine their speed and direction of travel, making this conventional SA capability extremely valuable for tracking mobile targets and increasing incentives for preemptive action.[25]

## *Entanglement*

Strategic SA can introduce escalatory risks along the entanglement pathway when parties to a crisis or conflict are unable to delineate between nuclear and conventional risks, thereby increasing the risk of miscalculation and unintended escalation. This can happen when conventional SA systems intentionally or unintentionally collect information on nuclear assets or when dual-use SA systems become military targets during a conventional conflict. Entanglement can also lead to escalation by convincing one or more countries in a crisis that their nuclear assets are at risk.

Research to date on entanglement has focused on several risks associated with the comingling of conventional and nuclear forces that could lead to escalation: (1) dual-use delivery systems that can be armed with nuclear and non-nuclear warheads; (2) the comingling of nuclear and non-nuclear forces and their support structures; and (3) non-nuclear threats to nuclear weapons and their associated C3I systems.[26] This definition is expansive but fails to account for the significance of the overall strategic SA ecosystem that is emerging, which introduces additional entanglement concerns associated with methods and systems meant solely to increase one's own SA (or obfuscate an adversary's SA). While these actions have not traditionally been viewed as particularly escalatory (as increased SA has been understood to increase strategic stability), the increased comingling of conventional and nuclear systems means improving SA as it relates to a conventional conflict could prompt either party to believe the conflict has entered a more dangerous phase, one in which the use of nuclear weapons (or an attempt to pre-empt their use) is possible.

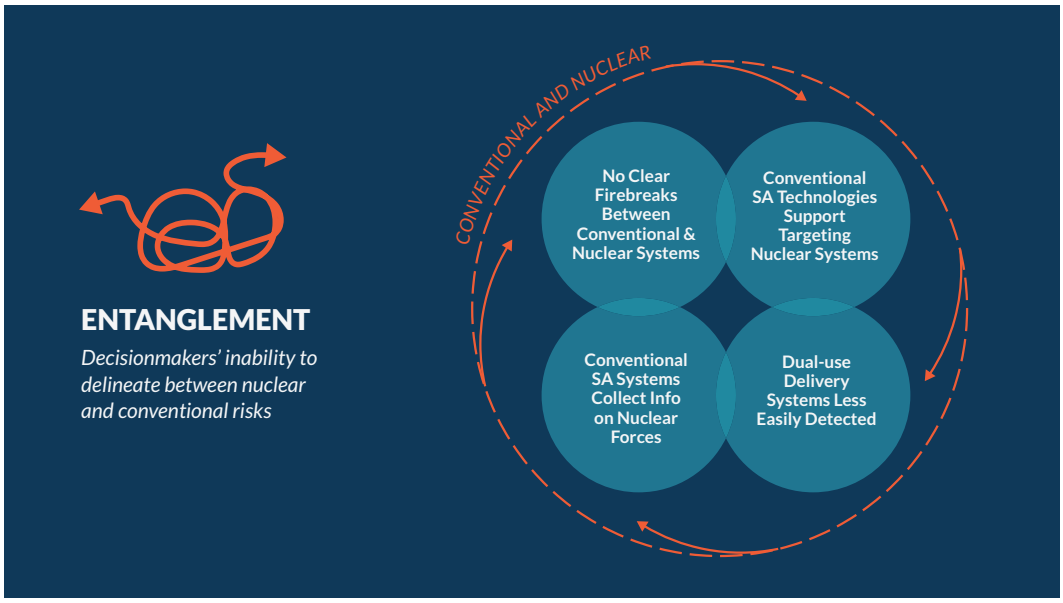
### STRATEGIC SA ENTANGLEMENT THREATS

More specifically, there are four major reasons this entanglement in the strategic SA ecosystem could lead to escalation. These are:

1. The emerging strategic SA ecosystem does not have clear firebreaks between conventional and nuclear systems, including for strategic warning and communications;
2. Conventional SA technologies are increasingly able to support targeting of nuclear/strategic systems;
3. Conventional/dual-use delivery systems are less easily detected and have less warning, therefore creating a growing desire for pre-launch warning; and
4. In crisis or conflict, conventional targeting of conventional strategic SA-related assets, especially if linked to command and control (C2) or decisionmaking, may still raise strategic escalation risks.

These risks can be overlapping and are not mutually exclusive. Comingled nuclear and conventional systems run the risk of exacerbating any number of these scenarios, and decisionmakers may decide against employing capabilities to avoid misinterpretation. Increasingly, however, as competition between nuclear-armed states continues, these four aspects of the strategic SA environment can play a role in determining how conflicts escalate.

Figure 4.2




First, the emerging strategic SA ecosystem lacks physical firebreaks, or tripwires, between conventional and nuclear systems, including for strategic warning and communications that might counter or disrupt escalatory pressures. This is significant as the dual-use nature of such capabilities means attacks on a warning or communications capability for strictly conventional purposes could be misconstrued as an effort to "blind" the target before launching a nuclear strike.

A major component of the strategic warning infrastructure for the United States is the array of satellites that can provide warning of nuclear launches and detect nuclear detonations. Until the mid-1980s, early-warning satellites employed by the United States were used exclusively for detecting the launch of nuclear missiles.[27] Similarly, the Air Force Technical Applications Center (AFTAC), the U.S. military organization that historically focused almost entirely on following Soviet nuclear weapons development, used satellites designed exclusively to detect nuclear explosions in the atmosphere or space until the 1980s, after which it began piggybacking on satellites deployed for other purposes.[28] Since then, motivating factors such as cost and flexibility have prompted the move toward using the same platforms for conventional tasks as well. For example, the U.S. Space-Based Infrared System (SBIRS) is a constellation of integrated satellites that enables such varied missions as providing early missile warning, cueing missile defenses, delivering technical intelligence, and supporting SA.[29]

Over the course of a conventional conflict between the United States and an adversary with ASAT capabilities, the use of such capabilities against dual-use satellites that provide early-warning functions would threaten escalation, as intentions would be difficult to discern. For example, some Chinese experts have argued that during a hypothetical conventional war with the United States, China should consider taking action against U.S. early-warning satellites to ensure the efficacy of conventional missile strikes against regional targets, an action that could be misinterpreted as an attempt to undermine the U.S. capacity to intercept Chinese ICBMs launched against the U.S. homeland.[30] Even if China has no intention of launching ICBMs against the U.S. homeland in this scenario, the perception associated with disabling or destroying an early-warning satellite could be highly escalatory, as decisionmakers would have reduced strategic SA throughout the scenario.

*The U.S. Air Force's 45th Space Wing supported United Launch Alliance's successful launch of the third Space Based Infrared Systems Geosynchronous Earth Orbit spacecraft aboard an Atlas V rocket from Launch Complex 41 here Jan. 20 at 7:42 p.m. ET.*

United Launch Alliance

The second risk for entanglement in strategic SA concerns the ability of conventional SA capabilities to support the targeting of nuclear forces and their support systems. Whereas the traditional command, control, surveillance, and warning systems focused either on nuclear warning ("nuclear" strategic SA systems) or on providing intelligence to commanders about the conventional battlefield ("conventional" strategic SA systems), today's dual-use strategic SA capabilities may be tasked to conduct both missions. This blurring effect between the conventional and nuclear potentially creates nuclear missions for what were previously considered conventional capabilities. For example, the RQ-4 Global Hawk is intended "to support joint combatant forces in worldwide peacetime, contingency and wartime operations" against a range of high value targets.[31] As Keir Lieber and Daryl Press suggest, increasingly capable UAVs like the Global Hawk, with advanced stealth and sensor capabilities, may also be useful to track a small country's mobile missiles, be they nuclear or conventional.[32]

Another conventional SA capability that could improve targeting of nuclear systems is non-acoustic submarine detection, which could be used to track both an adversary's conventional-only attack submarines as well as nuclear-armed SSBNs. Using light-based imaging or magnetic detection instruments, detection efforts have the potential to expose the location of SSBNs—capabilities that derive strategic significance from their ability to covertly maintain a second-strike capability.[33] If these SSBNs were targeted during a crisis using such detection methods, the surveilled state may believe the sea leg of their nuclear deterrent was compromised, potentially creating unintentional escalation.

*The Ohio-class ballistic missile submarine USS Pennsylvania (SSBN 735) transits the Hood Canal as the boat returns to its homeport at Naval Base Kitsap-Bangor, Wash., following a routine strategic deterrent patrol Dec. 27, 2017.*

U.S. Navy photo by Mass Communication Specialist 1st Class Amanda R. Gray

Advances in conventional and dual-use delivery systems have precipitated the third risk of entanglement in strategic SA in which weapons like hypersonic and cruise missiles are less easily detected and validated with traditional missile warning systems, creating a desire for more precise and widespread warning systems and pre-launch surveillance, with implications for both conventional and strategic conflict. For example, hypersonic weapons (both hypersonic glide vehicles and hypersonic cruise missiles), long-range traditional cruise missiles, and other capabilities are designed to elude traditional U.S. early-warning systems (i.e., radars and satellites), reduce confidence in warning, and defeat U.S. missile defenses. Traditional ballistic missiles leave the atmosphere and follow an unpowered trajectory before reentering the atmosphere toward a predetermined target. Missile defense systems, including Ground-based Midcourse Defense, rely on an advanced network of land, sea, and space sensors as well as ground-based interceptors that work together to track and target potential threats.[34] Hypersonic weapons aim to challenge detection and defenses using their speed, maneuverability, and low-altitude flight trajectory.[35] To counter these new delivery systems, the United States may have to rely on conventional SA systems, including systems that are more visible or dual use, to complete strategic missions and supplement strategic surveillance warning.

In addition, missile defense capabilities are viewed by some as having potential dual-use purposes. For example, China strenuously objects to the U.S. deployment of Terminal High-Altitude Area Defense (THAAD) missile batteries and their accompanying radar systems in South Korea. In this context, THAAD is primarily a missile defense system with a stated goal of intercepting North Korean short-range ballistic missiles using interceptors with a range of 200km.[36] However, its deployment has alarmed Beijing. Public statements suggest the Chinese government is concerned about potential uses of the AN/TPY-2 radar deployed with THAAD, fearing it could be used to gather information about its missile tests (both conventional and nuclear-capable) and other military operations, thus weakening the credibility of China's nuclear deterrent.[37] If an adversary were to feel threatened in a crisis and target such systems, would such an attack be considered conventional or strategic in intent and implication?

The final risk associated with entanglement is that of conventional targeting of conventional strategic SA-related assets that can nevertheless cause strategic escalation. As strategic SA systems become more networked and dual use, the threat of conventional attacks on them become more escalatory because states employing the capability are unable to determine if the attack is intended to degrade their conventional war-fighting capacity or their nuclear capacity. This escalatory threat is heightened if the conventional strategic SA is associated with C2 or decisionmaking activities. Examples of such threats include the networks of satellites employed by various states for dual-use purposes. The United States, for instance, has never fielded communication satellites used exclusively for nuclear operations.[38] While these satellites may have previously been perceived as impervious to adversary disruption, advances in ASAT capabilities may render these systems vulnerable. Satellite jamming, a conventional electronic attack that interferes with communications travelling to and from a satellite, runs the risk of leaving a targeted state strategically blinded, which could lead to "misinterpreted warning."[39] Although jamming ASAT capabilities have temporary effects (as the signal can be turned off and thereby restore adversary communications), states have strong incentives to target C2 warning and surveillance systems early in a crisis in order to ensure conventional dominance, intentionally or unintentionally threatening nuclear-related systems as well.

In addition to the space domain, computer networks that provide strategic SA can be dual use and are at risk of this type of escalatory threat. By employing an invasive cyber capability to collect information on an adversary's systems, actions, or intent, the very nature of that collection could trigger an escalatory response. For example, developments in cyberwarfare and electronic warfare have the potential to threaten previously secure strategic SA capabilities: Chinese experts believe the U.S. government is exploring the option of using cyber weapons to undermine adversary C2 during a crisis to prevent missile launches.[40] Even if the intent is not to sabotage nuclear systems but rather collect information (on either conventional or nuclear capabilities), the perception is what matters, and collecting information could prompt the target state to escalate a crisis if it fears its nuclear deterrent is compromised.

## STRATEGIC SA AND ENTANGLEMENT: NO LOOKING BACK

This new, increasingly complex, and integrated technology ecosystem provides clear benefits for both conventional and nuclear systems while simultaneously complicating the ability of decisionmakers to delineate between these dual-use purposes during a crisis or conflict. For the United States, prosecuting any type of conventional war without the extensive use of such capabilities and the information dominance they provide is unimaginable. This combined ecosystem may increase the risk of miscalculation and unintended escalation, as nuclear-armed adversaries face difficulty navigating crises while holding the risk of nuclear escalation at bay. In this way, the strategic SA ecosystem not only introduces new entanglement challenges, but these escalatory risks may also be less easily mitigated by strategies to "disentangle" or separate these capabilities given their essential and multipurposed roles early in crisis. These roles may even prove "indivisible."

Moving forward, the highly networked nature of conventional systems, as well as the dual-capable nature of many of them, may increase the potential for conflict to bleed from the conventional into the nuclear realm. Technical firebreaks have all but disappeared between many systems, opening the possibility that actions taken to gain information on conventional assets will be easily confused with more escalatory intrusions of nuclear-related systems. Historically, the conceptual validity of the "stability-instability paradox" was reinforced by distinct and stratified conventional and

strategic systems of warfare that amplified the division between strategic and conventional war. In a world in which these systems are increasingly dual use over the long term, the durability of that reassuring theoretical construct may be called into question, and new tools will be needed to replace the escalatory firebreaks that differentiated nuclear and conventional warning and surveillance systems that existed in the past.

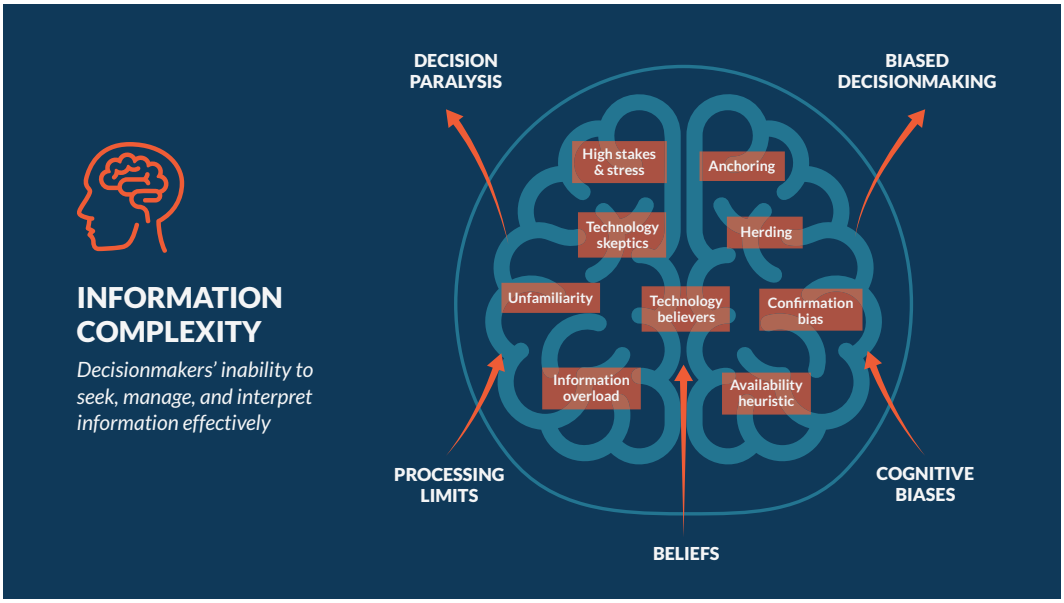
## *Information Complexity*

Emerging technologies for strategic SA have the potential to fundamentally transform the information domain and, if used effectively, to help decisionmakers manage crises more effectively with lower levels of risk. An important characteristic of the emerging strategic SA environment is the large volumes of data and information that is collected. The U.S. Air Force has defined this new information environment by four "Vs"—greater volume (collection of magnitudes more data points), greater velocity (the volume of data is acquired at extreme speeds), variety (numerous formats of information from diverse sources), and veracity (the volume, velocity, and variety of data includes a significant amount of noise and irrelevant data).[41] In a similar vein, the U.S. Navy has reported being overwhelmed by the floods of data generated from its existing information gathering systems. According to a RAND Corporation study, the amount of data being collected by the U.S. Navy increased at an exponential rate between 2000 and 2015.[42] Thus, information complexity describes the challenges decisionmakers' encounter as they seek, manage, and interpret information in this new environment.

Information complexity contributes to two potentially escalatory decisionmaking scenarios:

- **Decision paralysis:** the inability to make or finalize a decision in the time frame necessary, due to information overload or information shortfalls; and
- **Biased decisionmaking:** the excessive intrusion of belief or cognitive biases into the decisionmaking process in ways that diminish or discredit objective data and distort decisional outcomes.

Figure 4.3



These faulty decisionmaking outcomes result from the existence and interplay of several conditions, including cognitive processing limits, unacknowledged belief or value systems regarding information sources, and cognitive biases. The interaction of these factors may work to potentially impair effective crisis management and increase escalation risks. Processing limits, poor information management, and cognitive biases are longstanding risks in crisis management. However, the combination of increasingly complex information sources, unfamiliar technologies, and the high-stakes/high-stress nature of nuclear crises suggests that the escalatory risks associated with information complexity may be a growing concern.

## DECISION PARALYSIS

Information overload occurs when the volume of input to a system exceeds its processing capacity.[43] Critically, decisionmakers have limited cognitive processing capacity.[44] Emerging SA technology potentially can provide more accurate, detailed, and timely information that can help reduce ambiguity and differentiate credible information from the uncertain during a nuclear crisis. But this is only possible if the information can be organized, communicated, and absorbed effectively.[45] In addition to the quantity of information, the specific characteristics and quality of information can influence the degree of information overload as well.[46] Indeed, at the individual level, the development of new communication and information technologies has been recognized as an important factor in information overload.[47] Thus, in the emerging strategic SA ecosystem—where the volume, velocity, and variety of information have increased considerably and the veracity of information may at times be unclear—information overload is likely to become a more pronounced concern for decisionmakers.

For instance, distributed sensing platforms such as cubesats and swarmed unmanned vehicles may produce new streams of information to collectors and policymakers, complementing traditional data sources and providing needed confirmations of important observations. Miniaturization and improvements in networking are enabling the wide deployment of formerly limited capabilities, such as aerial full-motion video, and the exploitation of open sources, such as commercial satellite imagery and geographic information systems (GIS) data, all of which further increases information loads.[48] Combined with the data-mining capacity of cyber surveillance and the pattern recognition capacity of AI, the volume of information potentially available to enhance SA in a crisis is enormous. But if multiple data streams emerge with varying or divergent levels of confidence, decisionmakers may be overwhelmed with data or unable to differentiate data quality, especially if the provenance and validity of information cannot be demonstrably verified.

*U.S. Soldiers assigned to the 7th Special Forces Group conduct urban warfare training during Emerald Warrior 17 at Hurlburt Field, Fla., March 7, 2017.*

U.S. Air Force photo by Tech. Sgt. Barry Loo

The research is clear that increased information volume from SA technologies does not necessarily produce better decisionmaking. Indeed, when supply of information exceeds information-processing capacity, there is "widespread consensus" that performance is negatively affected.[49] At the individual level, information overload is linked with information anxiety and the inability to use relevant information to make a decision.[50] In the consumer context, individuals require more time to analyze information and reach a decision.[51] Similar experiments identify a range of cognitive and psychological effects whereby subjects tend to discard complex or conflicting information, settle for suboptimal conclusions to save time, and experience high levels of stress and other negative psychological effects.[52]

A recent study that measured performance of simulated C2 tasks with varying information volume and reliability found that increased volumes of task-relevant information did not improve task performance and led study participants to self-report reduced SA and interpersonal trust in their team members.[53] Upon encountering an overload of information with limited processing capacity, decisionmakers may face an impasse and fail to reach or communicate a decision. The failure to reach a decision advantages an adversary and could potentially result in further escalation. In a crisis, failure to reach a decision is a decision.

## BIASED DECISIONMAKING

Information overload and technology uncertainty or unfamiliarity also increase the influence of bias in decisionmaking. Overvaluing or undervaluing certain types and sources of information form part of the mental heuristics, or shortcuts, decisionmakers will use to discount or replace information sources in ways that are consistent with their beliefs.[54] Many decisionmakers have potent belief biases—both positive and negative—about the value and reliability of information and decision-support technologies.[55] This dynamic is prominently discussed in the context of AI, where the relative merits, reliability, and applicability of AI tools have been hotly debated and on which many policymakers have strongly-held views. This tension is best encapsulated by former Google CEO Eric Schmidt's 2018 statement, "[the] DoD does not have an innovation problem; it has an innovation adoption problem."[56] Decisionmakers tend to fall into one of two camps: the technology skeptics and the technology true believers.

The skeptics respond to new technologies with trepidation due to unfamiliarity and mistrust, which may make them discard information generated from emerging SA technology or fail to acquire enough information in the first place. This is especially acute with issues regarding the displacement of human decisionmaking with autonomous systems, machine learning, and AI. AI derives some of its unique advantages from being able to recognize patterns that human analysts cannot, but if the indicators that an AI system cites do not match a decisionmaker's idea of relevant indicators, they may dismiss it. AI systems may be seen as a "black box," making important decisions when few people outside of analytics teams, data science labs, and technology centers can fully understand how.

*The skeptics respond to new technologies with trepidation due to unfamiliarity and mistrust, which may make them discard information generated from emerging SA technology or fail to acquire enough information in the first place.*

Moreover, some technology resistance comes from the concern that decisionmakers will be

"black boxed"—forced to make decisions that must be publicly defensible or explainable based on information that is not.[57] AI is a principle source of concern in this regard, despite the fact that AI is expected to be particularly useful in collection.[58] Experts remain wary of relying on AI because AI systems cannot always explain how conclusions were derived and because the veracity of information can be difficult to judge. Senior decisionmakers are typically held accountable to the public and the institutions they lead for the decisions they make and are expected to explain and justify those decisions publicly to both domestic and international audiences.[59] However, this is difficult if the information on which the decision rests is not sharable or explainable. Moreover, when policymakers are bereft of a baseline understanding or grasp of AI, they will be unable to determine its practical limits and potential benefits.[60]

Reluctance to accept technology also stems from concerns about the vulnerability of technology to tampering or manipulation. Advances in autonomy and machine learning mean that a much broader range of physical systems are now susceptible to cyberattacks, including hacking, spoofing, and data poisoning. Similarly, machine learning-generated deepfakes (i.e., audio or video manipulation) have added a novel and potentially more sinister twist to the risk of miscalculation, misperception, and inadvertent escalation that originates in cyberspace but has a very real impact in the physical world.[61] Further, unmanned aerial systems may also fail due to multiple factors, including operator error, improper maintenance, loss of communication, equipment failure, and weather, among others. As the system matures, some causes of failure are largely mitigated (e.g., equipment failure), while other causes tend to persist (e.g., the risk of operator error).[62] Such qualms may make policymakers almost too cautious when deciding to deploy unmanned systems amid a crisis, creating information gaps and potentially heightening the risk that the United States and its allies could be surprised and disadvantaged during a conflict.

*Advances in autonomy and machine learning mean that a much broader range of physical systems are now susceptible to cyberattacks, including hacking, spoofing, and data poisoning.*

In stark contrast, risky belief biases run equally strong among the technology "true believers." These technology advocates are highly confident in given technologies and place considerable faith in the information they provide. In business psychology, this is known as the "technology effect," and research in this area suggests an implicit association between technology and success. Signals of high performance trigger the effect, and the effect is more likely when the technology invoked is unfamiliar.[63] One of the potential risks exacerbated by the complexity of data collection and analysis is the potential for analysts to operate on the faith that their systems yield appropriate insights. While SA technology has advanced to provide higher levels of detail and quality, this may contribute to a heightened degree of confidence in the information collected. However, the complexity of the technology hardware and software (e.g., distributed sensor networks with complicated information processing systems or AI systems with unexplainable algorithms) can make independent verification of the assessments obtained from these systems nearly impossible. The level of sophistication of emerging SA technology may lead to undue confidence in the assessments with no means for an independent cross-check.

Both technology skeptics and technology true believers risk engaging in biased decisionmaking by either accepting or rejecting information sets based on heuristics that seek to manage informational

*The level of sophistication of emerging SA technology may lead to undue confidence in the assessments with no means for an independent cross-check.*

complexity, both of which can exacerbate escalatory risks. If policymakers exhibit excessive caution from low belief in emerging SA technologies, they may reject or fail to obtain available information necessary for critically evaluating the positives and negatives of a preferred course of action and other alternatives. If an information search is perfunctory and incomplete, it fails to obtain several important pieces of information that may be crucial to defuse a crisis. While restraint is often perceived to be good, if it leaves policymakers in the dark, the opposite could also be true.[64] Although information dominance does not guarantee stability, its opposite—information inadequacy—may also serve to be an impediment to strategic stability.

## RELIANCE ON COGNITIVE BIASES

Belief systems regarding the role and utility of technology are by no means the only way biased decisionmaking can emerge in crisis scenarios. When problems include an unclear environment, an overload of data, lack of confidence in data sources, and lack of time for rigorous assessment of sources and validity, ambiguity may abet instinct and permit intuition to steer analysis. Potentially, the greater the ambiguity, the greater the likelihood that decisions will be driven by preconceptions.[65] Preconceptions could become a coping mechanism to simplify reality and mitigate information complexity. Cognitive bias—a challenge for all decisionmakers—may be exacerbated in the emerging strategic SA ecosystem where unfamiliar technologies or manifold sources of information are more prominent. In particular, perceptions of historical lessons from past crises that might have little relevance could also have outsized influence on decisionmakers who seek to ground decisionmaking in precedent and experience.[66]

*When problems include an unclear environment, an overload of data, lack of confidence in data sources, and lack of time for rigorous assessment of sources and validity, ambiguity may abet instinct and permit intuition to steer analysis.*

While a range of cognitive biases can be exacerbated by information complexity in crisis decision-making, overconfidence bias, confirmation bias, anchoring, and availability heuristic seem particularly challenging in these settings.[67] In the case of anchoring, psychologists have found that people tend to rely too heavily on the very first piece of information they learn, while discounting later information.[68] When it comes to emerging technology for SA, without a streamlined approach to deconflict a multiplicity of sources and with preconceived skepticism or unfamiliarity, decisionmakers may overvalue early sources rather than pursuing further options. Equally significant is the intrusion of confirmation bias—the tendency to search for, interpret, favor, and recall information in a way that confirms or strengthens one's prior personal beliefs or hypotheses. As described earlier, if a decisionmaker has low belief in an emerging SA technology, they may value evidence that supports this belief disproportionately to information that does not. This is particularly the case with AI: people are predisposed to view conclusions produced by humans as more transparent and explainable than those produced by AI-based methods but consistently overestimate the ability of humans to explain

their own deliberative processes.[69] Finally, the availability heuristic is a mental shortcut that relies on immediate examples that come to a person's mind when evaluating a specific topic, concept, method, or decision. The availability heuristic operates on the notion that if something can be recalled, it must be important, or at least more important than alternative information which is not as readily recalled.[70] Subsequently, under the availability heuristic, people tend to heavily weigh their judgments toward more recent or more memorable information and experiences, making new opinions biased toward that which can be more easily recalled.

One significant problem inherent to the aggregation of different information sources is the possibility that coincidental events will be misinterpreted. Escalated tensions over an individual issue could cause other, innocent actions to be perceived as aggressive or otherwise contribute to confirmation bias. Paul Bracken explores one historical example in detail: the connection between the Hungarian Revolution and Suez Crisis in 1956. In this case, unrelated events—Soviet fleet exercises involving transit through the Dardanelles, a British jet crash in Syria, and erroneous reports of Soviet troops movements by radar operators—coincided with heightened tensions over both incidents to give the impression of imminent Soviet intervention in Egypt.[71] In today's technology environment, such biases can be compounded by the integration of information streams and by efforts to supply information more directly and more quickly to policymakers via emerging strategic SA technology.[72]

## NAVIGATING INFORMATION COMPLEXITY

New research is examining promising ways in which training might reduce or mitigate the negative impact of cognitive biases and pre-held beliefs. Training may effectively debias decisionmakers over the long term.[73] In fact, experiments by Morewedge et al. (2015) find that interactive computer games and instructional videos can result in long-term debiasing at a general level. In a series of experiments, training with interactive computer games that provided players with personalized feedback, mitigating strategies, and practice reduced six cognitive biases by more than 30 percent immediately and by more than 20 percent as much as three months later. The biases reduced were anchoring, bias blind spot, confirmation bias, fundamental attribution error, projection bias, and representativeness.[74] The medical field is also recognizing the risks associated with decisional bias and seeking new training to reduce its negative effects on patient outcomes.[75] Research in medicinal debiasing emphasizes that experience in the field does not guarantee expertise, and debiasing for emerging technologies at more senior levels is sorely needed, since expert biases may run counter to next-generation scholars.[76] Fields as disparate as medicine and business are emphasizing the risks posed by biased decisionmaking and are developing tools to reduce them. Ultimately, their conclusions will prove equally relevant in national security crises between nuclear-armed states, where emerging technologies in a novel information space will engender problematic decisionmaking unless bias mitigation occurs.

## *Endnotes*

1 Robert Jervis and Mira Rapp-Hooper, "Perception and Misperception on the Korean Peninsula: How Unwanted Wars Begin," *Foreign Affairs*, June 2018, https://www.foreignaffairs.com/articles/north-korea/2018-04-05/perception-and-misperception-korean-peninsula.

2 John J. Mearsheimer, "Chapter 2: Anarchy and the Struggle for Power," in *The Tragedy of Great Power Politics*, 1st ed., The Norton Series in World Politics (New York, NY: Norton, 2001).

3 John H. Herz, *Political Realism and Political Idealism: A Study in Theories and Realities* (Chicago: University of Chicago Press, 1951).

4 Robert Jervis, "War and Misperception," *Journal of Interdisciplinary History* 18, no. 4 (1988): 675, https://doi.org/10.2307/204820.

5 Brian A. Jackson et al., *Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles* (Santa Monica, Calif.: RAND Corporation, 2008), https://www.rand.org/pubs/monographs/MG626.html.

6 Richard Leiby, "U.N.: U.S. Drone Strikes Violate Pakistan Sovereignty," *Washington Post*, March 15, 2013, https://www.washingtonpost.com/world/asia_pacific/un-us-drones-violate-pakistan-sovereignty/2013/03/15/308adae6-8d8a-11e2-adca-74ab31da3399_story.html.

7 Jim Garamone, "Iran Shoots Down U.S. Global Hawk Operating in International Airspace," U.S. Department of Defense, June 20, 2019, https://www.defense.gov/Explore/News/Article/Article/1882497/iran-shoots-down-us-global-hawk-operating-in-international-airspace/.

8 Donald J. Trump, Twitter post, June 21, 2019, 6:03 AM, https://twitter.com/realDonaldTrump/status/1142055375186907136.

9 Karsten Geier et al., *Moving Beyond Cyber Wars: A Translatlantic Dialogue* (Washington, DC: American Institute for Contemporary German Studies, Johns Hopkins University, September 2018), AICGS Policy Report, https://www.aicgs.org/2018/09/where-does-cyber-defense-stop-and-offense-begin/.

10 Robert Jervis, "On the Current Confrontation with Iran," War on the Rocks, January 9, 2020, https://warontherocks.com/2020/01/on-the-current-confrontation-with-iran/.

11 Geier et al., *Moving Beyond Cyber Wars*.

12 Robert Fanelli, "Cyberspace Offense and Defense," *Journal of Information Warfare* 15, no. 2 (2016): 53–65, https://www.jstor.org/stable/26487531?seq=1.

13 Tom Uren, Fergus Hanson, and Bart Hogeveen, "Defining Offensive Cyber Capabilities," International Cyber Policy Centre, Australian Strategic Policy Institute, July 4, 2018, https://www.aspi.org.au/report/defining-offensive-cyber-capabilities; and Gregory Rattray and Jason Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," in *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: National Academies Press, 2010), https://www.nap.edu/catalog/12997/proceedings-of-a-workshop-on-deterring-cyberattacks-informing-strategies-and.

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

15 Glenn Kent, Randall DeValk, and David Thaler, *A Calculus of First-Strike Stability* (Santa Monica, CA: RAND Corporation, 1988), https://www.rand.org/pubs/notes/N2526.html; Bell and Macdonald, "How to Think About Nuclear Crises."

16 Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1981), https://www.hup.harvard.edu/catalog.php?isbn=9780674840317.

17 Gregory H. Canavan, *Stability of Nuclear and General-Purpose Forces* (Los Alamos, NM: Los Alamos National Laboratory, 1997), http://library.sciencemadness.org/lanl2_a/lib-www/la-pubs/00412839.pdf.

18 Goldblum and Reddie, "Smallsats."

19 Sean Cate and Jesse Sloman, "Operating Under Constant Surveillance," *U.S. Naval Institute Proceedings* 142, iss. 5, no. 1,359 (May 2016), https://www.usni.org/magazines/proceedings/2016/may/operating-under-constant-surveillance.

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

21 Austin Long and Brendan Rittenhouse Green, "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy," *Journal of Strategic Studies* 38, no. 1–2 (January 2, 2015): 38–73, https://doi.org/10.1080/01402390.2014.958150.

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

23 Peter D. Feaver, "Command and Control in Emerging Nuclear Nations," *International Security* 17, no. 3 (1992/93): 165, doi:10.2307/2539133.

24 Vipin Narang, "War of the Words: North Korea, Trump, and Strategic Stability," Nuclear Security Working Group, n.d., https://nuclearsecurityworkinggroup.org/asia/war-of-the-words-north-korea-trump-and-strategic-stability/.

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

26 James Acton, ed., *Entanglement: Russian and Chinese Perspectives on Non-Nuclear Weapons and Nuclear Risks* (Washington, DC: Carnegie Endowment for International Peace, November 2017), https://carnegieendowment.org/2017/11/08/entanglement-chinese-and-russian-perspectives-on-non-nuclear-weapons-and-nuclear-risks-pub-73162.

27 Friedman, *Seapower and Space*, 242–245.

28 Krass, T*he United States and Arms Control.*

29 Missile Defense Project, "Space-based Infrared System (SBIRS)," Missile Threat, CSIS, August 11, 2016, last modified June 15, 2018, https://missilethreat.csis.org/defsys/sbirs/.

30 James Acton ed., *Entanglement: Russian and Chinese Perspectives on Non-Nuclear Weapons and Nuclear Risks.*

31 "Global Hawk Enterprise," Northrop Grumman, n.d., https://www.northropgrumman.com/air/global-hawk-enterprise/.

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

33 Evan Lisman, "Non-Acoustic Submarine Detection," *On the Radar*, CSIS, November 5, 2019, https://res.cloudinary.com/csisideaslab/image/upload/v1574455202/on-the-radar/Non-acoustic_Sub_Detection_Primer_c7ntof.pdf.

34 Missile Defense Project, "Ground-based Midcourse Defense (GMD) System."

35 Stephen M. McCall, "Defense Primer: Ballistic Missile Defense," Congressional Research Service, October 9, 2019, https://crsreports.congress.gov/product/pdf/IF/IF10541.

36 Missile Defense Project, "Terminal High Altitude Area Defense (THAAD)," Missile Threat, CSIS, June 14, 2018, last modified June 15, 2018, https://missilethreat.csis.org/system/thaad/.

37 Ethan Meick and Nargiza Salidjanova, "China's Response to US-South Korean Missile Defense System Deployment and Its Implications," United States-China Economic and Security Review Commission, June 26, 2017, https://www.uscc.gov/sites/default/files/Research/Report_China's%20Response%20to%20THAAD%20Deployment%20and%20its%20Implications.pdf.

38 Curtis Peebles, *High Frontier: The U.S. Air Force and the Military Space Program* (Washington, DC: Air Force Historical Studies Office, January 1997), p. 44–52.

39 Acton, "Escalation through Entanglement."

40 Fang Yong, "2015 年世界武器装备与军事技术发展重大动向" [Major trend of military equipment and technology development in the world in 2015], 军事文摘 [Military Digest], no. 23 (2015); and Deng Sijia, "美研发反导新技术：无人机发射激光 敌发射前打击" [U.S. develops new anti-missile technologies: UAV-borne laser and left of launch], PLA Daily, October 28, 2016.

41 Hamilton and Kreuzer, "The Big Data Imperative: Air Force Intelligence for the Information Age," *Air and Space Power Journal* 32, no. 1 (Spring 2018), https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-32_Issue-1/F-Hamilton_Kreuzer.pdf.

42 Porche et al., *Data Flood*.

43 Errol R. Iselin, "The Effects of the Information and Data Properties of Financial Ratios and Statements on Managerial Decision Quality," *Journal of Business Finance and Accounting* 20, no. 2

(January 1993), doi:10.1111/j.1468-5957.1993.tb00663.x.

44 Ibid.

45 Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable." *World Politics* 31, no. 1 (1978): 61-89. Accessed March 2, 2020. doi:10.2307/2009967.

46 Benjamin Schneider, "The People Make the Place," *Personnel Psychology* 40, no. 3 (September 1987): 437-453, doi:10.1111/j.1744-6570.1987.tb00609.x.

47 David Bawden, "Information and digital literacies: a review of concepts," *Journal of Documentation* 57, no. 2 (April 2001): 218-259, doi:10.1108/EUM0000000007083.

48 Hamilton and Kreuzer, "The Big Data Imperative."

49 Martin J. Eppler and Jeanne Mengis, "The Concept of Information Overload: A Review of Literature from Organization Science, Accounting, Marketing, MIS, and Related Disciplines," *Information Society* 20, no. 5 (November 2004): 325–44, https://doi.org/10.1080/01972240490507974.

50 David Bawden and Lyn Robinson, "The Dark Side of Information: Overload, Anxiety and Other Paradoxes and Pathologies," *Journal of Information Science* 35, no. 2 (April 2009): 180–91, https://doi.org/10.1177/0165551508095781.

51 Jacob Jacoby, "Information Load and Decision Quality: Some Contested Issues," *Journal of Marketing Research* 14, no. 4 (November 1977): 569, https://doi.org/10.2307/3151201; Jacob Jacoby, "Perspectives on Information Overload," Journal of Consumer Research 10, no. 4 (March 1984): 432, https://doi.org/10.1086/208981.

52 Eppler and Mengis, "The Concept of Information Overload"; Bawden and Robinson, "The Dark Side of Information"; Nathan McNeese, Verica Buchanan, and Nancy Cooke, "The cognitive science of intelligence analysis," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 59 (2005): 826–830, doi:10.1177/1541931215591250.

53 Marusich et al., "Effects of information availability on command-and-control decision making."

54 Cindy Dietrich, "Decision Making: Factors that Influence Decision Making, Heuristics Used, and Decision Outcomes," *Inquiries Journal/Student Pulse* 2, no. 2 (2010), http://www.inquiriesjournal.com/a?id=180.

55 Dima Adamsky, *The Culture of Military Innovation: the Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel* (Stanford, CA: Stanford University Press, 2010).

56 Eric Schmidt, "Statement of Dr. Eric Schmidt House Armed Services Committee April 17, 2018," Statement before the House Armed Services Committee, April 17, 2018, https://docs.house.gov/meetings/AS/AS00/20180417/108132/HHRG-115-AS00-Wstate-SchmidtE-20180417.pdf.

57 KMPG International Data and Analytics, *Guardians of trust: Who is responsible for trusted analytics in the digital age?* (Amstelveen, Netherlands: KMPG, February 2018), https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/02/guardians-of-trust.pdf.

58 Daniel S. Hoadley and Kelley M. Sayler, "Artificial Intelligence and National Security," Congressional Research Service, updated November 21, 2019, https://fas.org/sgp/crs/natsec/R45178.pdf.

59 Robert D. Putnam, "Diplomacy and Domestic Politics: The Logic of Two-Level Games," *International Organization* 42, no. 3 (1988): 427-60, www.jstor.org/stable/2706785.

60 Michael C. Horowitz and Lauren Kahn, "The AI Literacy Gap Hobbling American Officialdom," War on the Rocks, January 14, 2020, https://warontherocks.com/2020/01/the-ai-literacy-gap-hobbling-american-officialdom/.

61 James Johnson and Eleanor Krabill, "AI, Cyberspace, and Nuclear Weapons," War on the Rocks, January 31, 2020, https://warontherocks.com/2020/01/ai-cyberspace-and-nuclear-weapons/.

62 Christopher W. Lum and Blake Waggoner, "A Risk Based Paradigm and Model for Unmanned Aerial Systems in the National Airspace," American Institute of Aeronautics and Astronautics, 2011, http://faculty.washington.edu/lum/website_professional/publications/Lum_UAS_risk_2011.pdf.

63 Brent B. Clark, Christopher Robert, and Stephen A. Hampton, "The Technology Effect: How Perceptions of Technology Drive Excessive Optimism," *Journal of Business Psychology* 31 (2016):

87-102, https://doi.org/10.1007/s10869-015-9399-4.

64 Robert Jervis, *Perception and Misperception in International Politics: New Edition* (Princeton, NJ: Princeton University Press, 1976), doi:10.2307/j.ctvc77bx3.

65 Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable."

66 Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," Science 185, no. 4157 (September 1974): 1124-1131, https://www.jstor.org/stable/1738360.

67 Department of Home Affairs, *Decision Making During a Crisis: A Practical Guide* (Canberra, Australia: Government of Australia, 2018), https://www.organisationalresilience.gov.au/resources/Documents/decision-making-during-a-crisis-a-practical-guide.pdf.

68 Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011).

69 Molly Kovite, "I, Black Box: Explainable Artificial Intelligence and the Limits of Human Deliberative Processes," War On The Rocks, 2019, https://warontherocks.com/2019/07/i-black-box-explainable-artificial-intelligence-and-the-limits-of-human-deliberative-processes/.

70 Daniel Kahneman and Amos Tversky, "Availability: A heuristic for judging frequency and probability," *Cognitive Psychology* 5, no. 2 (September 1973): 207-232, https://doi.org/10.1016/0010-0285(73)90033-9.

71 Ibid.

72 Paul Bracken, "Instabilities in the control of nuclear forces," in *Breakthrough: Emerging New Thinking—Soviet and Western Scholars Issue a Challenge to Build a World Beyond War*, Anatoly Gromyko and Martin Hellamn, eds., (New York, NY: Walker & Company, 1988).

73 C. K. Morewedge et al., "Debiasing Decisions. Improved Decision Making With A Single Training Intervention," *Policy Insights from the Behavioral and Brain Sciences* 2, no. 1 (2015): 129-140, https://openaccess.city.ac.uk/id/eprint/12324/1/Debiasing_Decisions_PIBBS.pdf.

74 Ibid.

75 T. D. Wilson and N. Brekke, "Mental contamination and mental correction: unwanted influences on judgments and evaluations," *Psychological Bulletin* 116, no. 1 (1994): 117–142, doi:10.1037/0033-2909.116.1.117.

76 Pat Croskerry, Geeta Singhal, and Silvia Marnede, "Cognitive debiasing 1: origins of bias and theory of debiasing," *BMJ Journals* 22, iss. supp. 2 (September 2013): ii58-ii64, https://qualitysafety.bmj.com/content/22/Suppl_2/ii58.full.