Strategic Studies Quarterly

Attribution and Operational Art: Implications for Competing in Time

Lt Col Garry S. Floyd Jr., USAF

Abstract

The world is wired with networks and unblinking sensors that track everything from spending habits to the movements of armies. Yet, despite the proliferation of data, attribution remains an enduring problem. A plane crashes into a building. A nuclear physicist dies under mysterious circumstances. So-called fake news spreads disinformation across social media on the eve of an election. These things happen and too often the world is left with questions about who to hold accountable. Decision makers need a way to assess attribution problems caused by adversaries, while also identifying and understanding opportunities when they hold and might utilize an attribution advantage. This article offers a model that visualizes attribution decisions and their associated risks at the operational and strategic echelons of command. The model is tested across three mini-case studies. What emerges in the analysis is a novel approach planners can use in considering covert operations, an approach that better accounts for the attribution problems inherent to operations in the cyber domain. The results of the analysis further suggest that properly leveraging attribution advantage creates opportunities for controlling the timing and tempo of military operations. Finally, this article presents several recommendations about how attribution advantage can be pursued at lower echelons in multi-domain operations that may offer some defense against attribution problems imposed by adversaries.

✵✵✵✵✵

Lt Col Garry S. Floyd Jr. currently serves on the Algorithmic Warfare Cross Functional Team within the Office of the Undersecretary of Defense for Intelligence. He is a career intelligence officer and former intelligence squadron commander. Floyd holds several masters degrees, including international relations (Troy University), military art and science (US Army School of Advanced Military Studies), and most recently, strategy and technology integration (Air University).

During a keynote speech to the Air Force Association in September 2016, Air Force Chief of Staff Gen David Goldfein described his vision of the future of warfare as the intersection of an effects grid, a sensing grid, and multi-domain command and control. He further stated that "if you take a look at the effects grid, you have to create effects that are attributable, or not attributable. Sometimes I want them to know it's me, sometimes I don't."[1] General Goldfein offers a compelling perspective on the nature of modern and future war. Yet when one considers airpower and the US Air Force the images that most likely come to mind are those of a fighter pilot straining against gravity through difficult maneuvers or a bomber crew tirelessly flying long-range strike missions across the globe. Why, then, did the senior ranking general in the world's most powerful air force make reference to "non-attributable combat capabilities and effects?

The answer lies in understanding the role that attribution might play in operational art, and specifically, how attribution can help one side gain an advantage in the dimension of time. Attribution is defined here as the act of "ascribing agency to an agent."[2] Whenever anything terribly bad or wonderful and good happens human nature demands an answer about whom to hold responsible, whom to reward, or whom to punish.

In operational art, attribution can be a tool well suited to the task of dominating the dimension of time. Time refers to that human-made construct that influences nearly every aspect of society by measuring the relationship between events. Seeking advantage in the dimension of time can be defined as diplomatic and military efforts designed to influence or disrupt decision cycles of opponents to gain more time or control the timing of events. Military theorist John Boyd envisioned weapons and operational concepts that could "simultaneously compress" time for one side while stretching it out for the other to "generate a favorable mismatch in time (and) the ability to shape (an environment) and adapt to change.[3] So where is the crossroad of attribution, Boyd's pursuit of advantage in time, and an emerging focus on military operations across multiple domains?

The promise and prominence of war fighting in the cyber domain is one part of the answer, but there is a broader context, also reflected in General Goldfein's message, that speaks to the enduring nature of war. Despite every attempt to thwart them with technology, the basic elemental forces of war—uncertainty, friction, and chance—still loom over the battlefield, menacing even the best laid plans. With proper planning and execution, non-attributable effects are possible in every war-fighting domain. There is diversity in non-attributable effects. It can be cognitive, logical, or physical in nature. In this sense, non-attributable effects might include covert aerial drone strikes, difficult-to-trace offensive cyberattacks, special operations forces operating deep in another country, or information attacks designed to undermine rival governments.

Attribution advantage occurs when one party in a conflict creates a military effect and then intentionally and successfully exercises influence over the detection and attribution of that effect while thwarting similar efforts from adversaries. This article first explores the cognitive terrain where uncertainty thrives despite increasingly persistent intelligence sensors. Next, it briefly reviews existing military doctrine on deception and considers the relationship between deception and attribution. Then the article offers a model that provides a method for evaluating when nonattributed effects should be pursued, when self-attribution might prove beneficial, and the implications for both. Self-attribution in this context occurs when a party takes credit, or perhaps blame, for an action that they may or may not have taken. The potential utility of the model offered in this paper is evaluated in three mini-case studies as notional examples: Putin's invasion of Crimea, US support for the Afghan mujahideen during the Soviet occupation of Afghanistan, and the dramatic events surrounding the Sony Pictures hack. What emerges is that attribution advantage—for those who can gain it—offers opportunities in the contest for time, but not without serious implications that must be considered and accounted for in planning. Boyd sought to "collapse (an) adversary's system into confusion and disorder by causing him to over- and underreact to activity that appears simultaneously menacing as well as ambiguous, chaotic, and misleading."[4] The concept of attribution advantage supports those aims.

Attribution and the Cognitive Domain

Attribution problems are rooted in the cognitive domain, that space in the minds of commanders where facts and fears contest for decision. While many scholars, observers, and practitioners have attempted to frame the immense cognitive challenges of war, none have done so with more impact than Carl von Clausewitz. Uncertainty and friction dominate in Clausewitz's depiction of war, looming insidiously to varying degrees behind nearly every decision in the prosecution of campaigns and battles. While Clausewitz never uses the phrase "cognitive domain," his words describe its nature. He wrote that "war has a way of masking the stage with scenery crudely daubed with fearsome apparitions" and that the "difficulty of *accurate recognition* constitutes one of the most serious sources of friction in war, by making things appear entirely different from what one had expected."[5] Clausewitz further elaborated about how new information tends to "trickle" in to the commander, making him "more, not less uncertain."[6] The stark reality of war in terms of the effects created by friction, uncertainty, fear, chance, and danger is precisely what makes attribution advantage so compelling.

Attribution advantage suggests that both strategic-level decision makers and operational-level commanders should give thought to attributing combat effects in multi-domain operations. There may be situations in which operational benefit might be had in purposeful self-attribution. Scenarios in which self-attribution causes adversaries to question entire information streams or data sources are one example. This might involve informing an adversary that their weather radars are no longer providing accurate storm tracking or that the facilities where they store fuel are no longer accurately measuring the amounts on hand. Informing an adversary that their command systems data is being tampered with may cause that adversary to lose trust in an information conduit or a source. A most likely and immediate result of doing so is that the adversary's decision processes will suddenly take longer as the adversary attempts to find decision data they can trust. Longer decision cycles expose the adversary to additional intelligence collection efforts and potentially enhance kinetic targeting. While self-attribution might mean sacrificing a capability, advantages in time can be found by surprising the enemy.

Clausewitz and Boyd frame war as a daunting mental endeavor given its violence and the consequences of failure. Perhaps the minds of decision makers may soon prove even more vulnerable to manipulation as an emerging conditions of warfare. The internet, by its very nature, aside from providing an effective conduit for non-attributable effects, may be magnifying decision makers' susceptibility to cognitive manipulation. Nicholas Carr takes on the task of understanding the internet's influence on mankind's collective ability to think critically in *The Shallows: What the Internet Is Doing to Our Brains.* Carr describes the internet as "an interruption system," and his findings suggest that the internet is making it both practically and physiologically more difficult for humans to think deeply about problems.[7] This does not bode well for the human species writ large, much less the military commander. Daniel Kahneman, in *Thinking, Fast and Slow* and in numerous other publications, has explained the myriad number of ways in which the human mind is already primed to reach incorrect conclusions from hastily assimilated data.

Kahneman challenges the notion that actors in a political or economic arena behave rationally and therefore predictably by unveiling a litany of shortcomings and biases. He does this by describing human thinking as happening in two separate and distinct systems. The first he dubs "System 1" thinking that "operates automatically and quickly," which is opposite from "System 2" thinking that is more deliberate and useful in complex situations.[8] Kahneman demonstrates that human failings are often the result of heuristic processes employed in System 1 thinking to reach expedient solutions. Indeed, he offers an entire lexicon of heuristic practices that can lead to cognitive inspired failings. One particularly powerful idea is his WYSIATI concept, an acronym for What You See is All There Is.[9] Kahneman asserts that in System 1 thinking, "the measure of success is the coherence of the story it manages to create. The amount and quality of the data on which the story is based is largely irrelevant."[10] When the battlefield is the mind of an enemy commander, System 1 and System 2 thinking become new avenues of approach in key terrain.

Indeed, taken together, Kahneman and Carr's portrait of the cognitive domain suggests that the human mind is increasingly vulnerable to attack despite the digital assistants making their way into every modern home. The minds of decision makers are no less vulnerable, despite their assumed access to exquisite sources of intelligence. Non-attributable effects, or effects generated with the intent of eventual and purposeful self-attribution, magnify uncertainty. An operational objective might be to maximize uncertainty to push adversary decision makers from System 1 to System 2 thinking for the purpose of expanding decision time. Another line of operation might include covertly inserting data that blends in with the background data fueling the adversary's shallow System 1 thinking. Still another method might involve finding ways to alter command signals moving from the headquarters to the field. Subordinates reserving their System 2 thinking for other tasks may prove vulnerable in cultures where questioning orders from higher echelons is not encouraged.

Attribution and Deception

Vulnerabilities inherent within the cognitive domain suggest that the attribution problem has its basis in deception. Deception is prerequisite for attribution advantage whenever or wherever detection cannot be avoided. For example, perhaps one generates an affect that its adversary is not only unaware of but remains unaware of until some critical moment when it discovers that a critical capability is suddenly impotent or providing inaccurate data. At that moment, when the adversary discovers an effect, subterfuge about who is responsible fuels attribution advantage and preserves flexibility for the aggressor. Another possibility is that the target is made aware of the effect by its adversary but not its author, and the proffered symptoms of the problem lead the target toward attributing the source of the problem to other causes. Machines, in fact, do sometimes break down and humans in the loop are always prone to error. The advantages an operational artist derives from these opportunities hinge upon deception. In many of these scenarios, where detection is rightly presumed to be only a matter of time, someone or something is always being lied to or misled. In those moments, the information streams upon which decisions are made are polluted and unsafe. When stealth enables a non-attributable effect, the adversary does not even know not to trust their systems, data, or processes for as long as detection is delayed.

Deception is fundamental to generating non-attributable effects. There is always some element of deception at work, even in those instances where the introduction of deceptive or false information is not the primary goal of the operation. While current joint doctrine on military deception does not directly address the pursuit of attribution advantage, it does provide guidance that seems applicable. There is an action element coded in joint military deception doctrine. The object of deception operations is not simply to mislead, but to force a desired outcome concerning the enemy. For example, US Department of Defense Joint Publication 3-13.4 defines military deception as actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.[11]

Achieving attribution advantage is a balance between positive and negative actions of both the party with initiative and the target of the desired nonattributed attack. Positive actions mean “doing something” while negative actions refer to one side or the other “not doing something.” For the party with the initiative, positive actions involve building a strong case for plausible deniability or leaving behind clues in the wake of an operation that lead an adversary to misattribute the cause of the effect. Again, for the party with the initiative, negative actions eschew active misdirection in favor of efforts aimed to achieve stealth. Whichever approach the operational artist pursues, the goal is to cause the adversary to make a bad decision, a positive action, or to perhaps miss a critical opportunity through negative action or inaction.

Joint doctrine explores the approaches to deception by introducing the concept of conduits to explain these various approaches. Conduits are defined as “information or intelligence gateways to the deception target. Conduits may be used to control flows of information to a deception target. It is rare that a deceptive message is sent directly to the deception target itself. Most often, deception messages are sent to intelligence collectors (conduits) with the expectation that the deceptive message will systematically make its way to the deception target.”[12]

While the concept of conduits seems sound and logical, joint doctrine seems to unnecessarily constrain the operational artist’s thinking. Indeed, in the near future, it may be common for actors with the initiative to send “deceptive messages” directly to decision makers. The question becomes one of just how directly and effectively that can be accomplished balanced against the perceived necessity for stealth and nonattribution.

However, it is worth noting that deception is a tool that is also available to defense. Eric Gartzke and John R. Lindsay point out that “if it is easy for a covert attacker to gain access to an organization’s data, it is also easy for a network protector to feed the attacker data that are useless, misleading, even harmful.”[13] If one considers attribution advantage as something to be won in the cognitive domain, and the contest between offensive and defensive efforts in deception, Boyd’s famous “OODA Loop” begins to look less like a theory about decision-making processes depicted in a wire diagram and more like a terrain map of targets in a contested battlespace.

Through the OODA Loop, Boyd explained basic decision making as observing, orienting, deciding, and acting upon information. SAF targeteers traditionally place red triangles on the targets upon which they desire to create effects. If one places a few triangles on the OODA Loop it begins to look like a map of physical space or perhaps a campaign map for the cognitive battleground (see figure 1). The small triangles indicate targets for the aggressor or traps the defender leaves open to its attacker. The result is that attribution becomes a question to be answered in the synchronization of effects in multiple war-fighting domains, for all of the parties involved in the conflict.

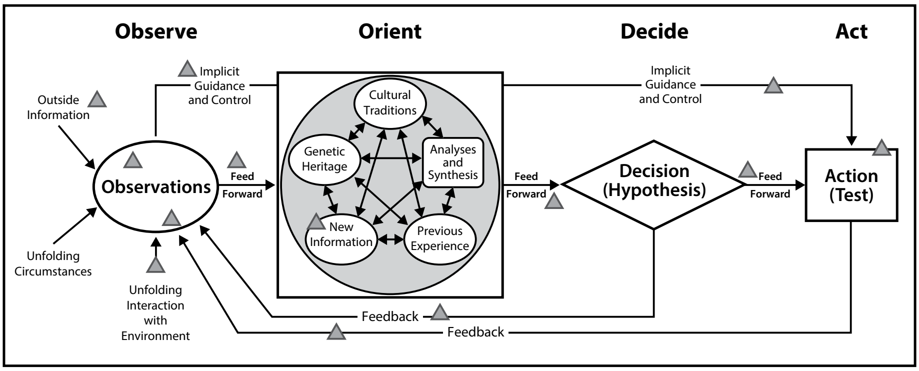


Figure 1. Boyd's final OODA-loop sketch. (Adapted from Grant Tedrick Hammond, *The Mind of War: John Boyd* and *American Security* [Washington, DC: Smithsonian Institution Press, 2001], 190.)

Operational Art and Attribution Advantage

Clausewitz described the atmosphere and the challenges inherent with the cognitive domain. However, Sun Tzu's guidance from over 2,000 years ago may be more relevant to the operational art of attribution advantage. Sun Tzu wrote, "War is the art of deceit. Therefore, when able, seem unable; when ready, seem unready; when nearby, seem far away; and when far away, seem near . . . if [your opponent] is humble, encourage his arrogance . . . if he is internally harmonious, sow divisiveness in his ranks. Attack where he is not prepared; go by way of places where it would never occur to him you would go."[14]

Sun Tzu's contribution to military thinking and strategy is the art and practice of indirect warfare. Winning without fighting still means winning. The terms by which the desired result is achieved are simply different. The mindset that accompanies indirect warfare is useful in considering warfare in the cognitive domain and the exploitation of attribution advantage.

Boyd drew some important distinctions between the approaches taken by Clausewitz and Sun Tzu to warfare in the cognitive domain. He suggested that Clausewitz "failed to address the idea of magnifying an adversary's friction and uncertainty."[15] Further, Boyd's understanding of Sun Tzu is that commanders should seek opportunities to "shape the enemy's perception of the world to manipulate his plans and actions."[16] That understanding is reflected in Joint Publication 3-13.4 in that the purpose of deception operations should be to cause the enemy to either do or not do something tangible, rather than simply to make the enemy think something. Considering the pursuit of attribution advantage as a cognitive avenue of approach suggests an indirect method for setting conditions for the conflict, such as the timing and location.

To pursue a nonattributed effect, or to self-attribute an effect previously undetected or unattributed by an adversary, is to seize the initiative in the cognitive domain. The questions that now emerge turn upon operational utility, risk, planning, and execution. The answers may be found in the measures of effectiveness by which the risk and operational utility of attribution advantage might be assessed. Defining those measures of effectiveness can be thought of as establishing the questions decision makers and planners should ask prior to execution. Some of these questions include:

How much damage will this attack cause to the targeted system?

The question of damage is not trivial. The amount of damage done may correlate directly to the adversary's response. Further, given the rise of social media, the impact of operations on public opinion is felt sooner, providing just-war traditions like proportionality with new strength.

How long until the adversary detects something is wrong in the targeted system that is, how long before effects become visible or measureable?

Regardless of the domain in which effects are created, detection of effects by an adversary starts the clock on the adversary's response. In a seminal work on covert actions, Gregory Treverton wryly asserts that covert operations are always eventually discovered.[17] If taken as truth, delaying detection is the first order for the side with initiative. Preventing or delaying attribution becomes the challenge upon discovery.

What is the likelihood this operation might cause unintended damage?

Some authoritarian regimes seem to have developed an immunity to the concept of collateral damage. However, for most, the question of unintended damage is crucial, particularly when nonattributed effects are the goal. The political consequences of severe collateral damage can only be magnified when they occur during the execution of a covert operation.

Is plausible deniability feasible?

Recently the leader of a nuclear-armed nation was able to foster ambiguity and maintain a semblance of plausible deniability in an era of constant coverage by both the media and intelligence sensors. Further, disinformation branded as "fake news" seems to have given new life to an old concept. Plausible deniability places the burden of proof on the accuser. An intelligence service may have evidence of an offense committed by an actor, but whether policy makers can use that to publicly make their case without compromising sensitive sources and methods is always in question. Of course, plausible deniability is not necessarily an easy path for the would-be attacker. Joseph Nye points out that an "attacking government or non-state actor knows what its role was, but it cannot be sure how good the opposing forensics and intelligence are."[18] Nye's focus was on deterrence in cyberspace, but the statement stands for other covert actions as well.

What is the assessed ability to shape attribution toward another actor?

The truism that perception is reality holds sway, and circumstantial evidence can be thought of as camouflage for the mischievous. When two parties are in conflict, it provides near perfect cover for a third party to skillfully exploit the situation, whatever the motivations. False-flag attacks, where assailants disguise themselves as another, should be expected.

How vulnerable are one's own interests should a tool, asset, or operation be discovered?

This is particularly relevant in the cyber domain. Before an elegant cyberattack is unleashed on some unsuspecting adversary, one should first explore the possible implications if the weapon is discovered and then repackaged and redirected against its creators.

What attribution resources might an adversary bring to bear once an effect is discovered?

Some actors simply have more capabilities to apply against an attribution problem than others. However, an aggressor should always bear in mind that when something "new" is observed, whether in the physical or the digital realm, the discovery draws attention from those seeking either to understand it, counter it, or replicate what has been found.

Modeling Attribution

The model represented by the spider chart in figure 2 is offered to address these questions by providing a graphical depiction of the operational utility and risks of weaponizing attribution under various conditions. The attribution advantage model provides seven vectors upon which to measure the merits of attribution. It provides a method for framing the opportunities and risks associated with pursuing nonattributed effects and whether one should self-attribute an effect or capability that might otherwise have remained stealthy. The model is meant to help an operational commander or decision leader better understand when they have an attribution advantage and guide their thinking about how and when they should use that advantage.

For the purpose of introducing the model, three conditions are set in figure 2, and in each the assumption is that the desired effect can be achieved with the highest possible confidence. In practice, scoring within the model will always be somewhat subjective, as scoring is necessarily based on the best available all-source intelligence on the adversary's capabilities and situation, as well as one's understanding of one's own capabilities (see appendix for further discussion of scoring). Further, it is once again important to note that this model is not meant solely for the cyber domain. The model is intended as a means to analyze the attribution question across the range of covert capabilities, from cyberattacks to stealthy air strikes and special operations employment.

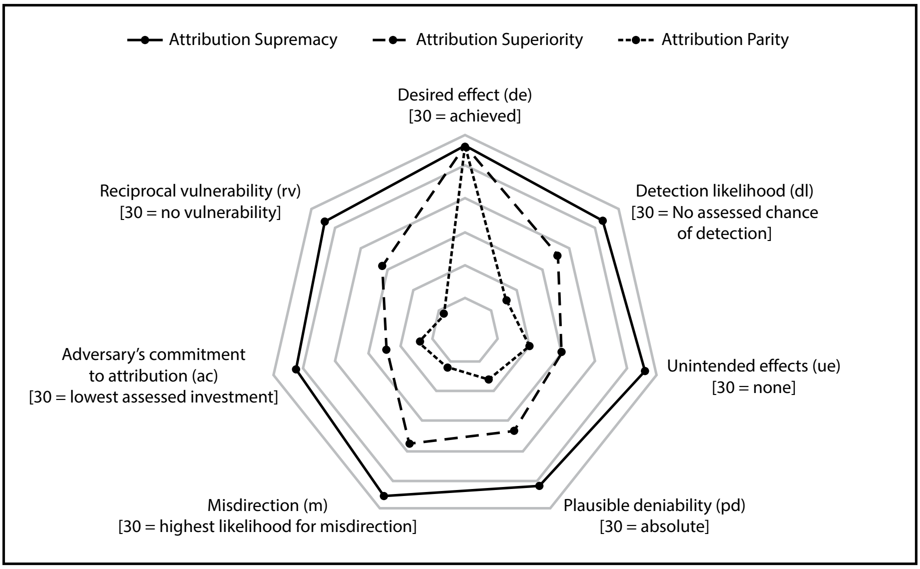


Figure 2. The attribution advantage model

Borrowing from airpower doctrinal terms, the highest tiered condition is "attribution supremacy." Under conditions of attribution supremacy, the aggressor possesses a weapons platform, tool, or capability that achieves the desired effect with little chance of detection and little chance of causing unintended effects. In a scenario where attribution supremacy exists, the aggressor is highly certain of its ability to maintain plausible deniability, is confident that it can misdirect attribution toward another party or cause, and has taken steps to ensure that it is invulnerable to the attack it is about to unleash on its opponent. Further, the party with the initiative assesses that its target will dedicate minimal resources to discover attribution, either by choice or because of resource scarcity. In conditions of attribution supremacy, incentives for aggressors to conduct operations designed to produce non-attributable effects are very high. The party with initiative is also in position to control the timing of attribution. If decision makers and planners sense an advantage in self-attribution, they can do so given their limited vulnerability to a reciprocal attack and the lack of unintended consequences for which they might be held accountable. Finally, under conditions of attribution supremacy, the assailant is highly confident it can attribute attacks intended to be non-attributable delivered by its enemy or interested third parties. That confidence might stem from exquisite access to adversary decision making or simply the ability to mass resources against attribution problems.

Sustained attribution supremacy may be difficult to maintain or even achieve. A more realistic objective for an aggressor might be "attribution superiority." Plausible deniability and successful misdirection are achievable—but more temporary. The advantage of preventing one's actions from being detected is more fleeting. Therefore accounting for the discovery of one's actions is more prudent during operational planning. Further, under conditions of attribution superiority, the ability to remain undetected may prove localized, meaning the target might remain unaware of an attack, but other interested parties may prove able to gather and process data suggesting that something is afoot. When a third party detects an act or an attack that they assume the perpetrator wishes to remain secret, they face an important series of questions. Do they attribute the act publicly, spoiling the apparent, perhaps temporary attribution superiority the aggressor had enjoyed? Do they covertly confront the aggressor conducting the act in pursuit of some profit or political advantage? Do they covertly inform the aggrieved party, again for some profit or advantage? Or do they simply remain quiet, preserving the ability to detect and attribute until some greater benefit might be had?

However, many scenarios are likely to more closely resemble "attribution parity," depicted in figure 2 by points plotted more toward the center of the graph. Risks abound under conditions of attribution parity. Perhaps the actor possesses a platform that is highly effective but is equally as vulnerable to the weapon, given the costs of preemployment inoculation or postattack remedy. Furthermore, under conditions of attribution parity, the development of a special capability might make it exquisitely complex and costly to produce. This might frustrate plausible deniability or technical efforts to misdirect attribution. Lindsay suggests "the increasing costs of attack against valuable targets [offer] some hope that strategies of denial can protect vital systems. The vulnerability of anonymous attackers to compromise in the most complex targets also offers some hope for deterrence strategies."[19] Lindsay primarily focuses on the attribution problem in the cyber domain, but his statement holds true across domains. The employment of an exquisite capability limits the possible number of responsible actors, as high-value targets are often the most well defended.

Still another problem for the side seeking to go on the offensive under conditions of attribution parity are the unintended effects that a covert operation might have and the blowback that may result from discovery. Many reporters and scholars have focused on the Stuxnet computer worm, which comprised a highly sophisticated cyberattack that targeted Iran's nuclear facilities. If David Sanger's reporting is accurate, key US policy makers at the highest level did not demand assurances that the worm would not cause unintended damage until after it had begun spreading to unintended systems in cyberspace.[20] Unintended or collateral damage is no longer simply a concern for targeteers employing traditional bombs or cruise missiles.

The conditions found in attribution parity suggest the party attempting to seize the initiative has very little control over whether or not attribution occurs and may be vulnerable to an attack delivered via a similar platform. There is a high risk of detection, as the adversary is likely to invest significant resources to attribute the attack once the effect is discovered. Treverton puzzles over how decision makers seem to always believe that their covert operations will remain secret, despite ample evidence that suggests otherwise.[21] That said, if mitigation is available for the vulnerability problem, there may be scenarios at attribution parity where self-attribution should be considered as a means to control the narrative or to enhance one's future credibility for launching future attacks. Finally, attribution parity implies that one's adversary may be very capable of creating their own difficult-to-attribute effects. This creates conditions favorable to long, limited conflicts where the risk of sudden, uncontrolled conflict escalation is continually high.

Attribution Advantage in Practice: Putin, Ukraine, and Crimea

Vladimir Putin's Russia seems to have an implicit understanding of the political risks and benefits of attribution. Since 2013, Russia has reportedly been involved in military interventions and linked to offensive cyber actions in Syria, the Baltic States, Georgia, and Ukraine. In 2014, British Broadcasting Corporation (BBC) News captured a dilemma shared by the news media, scholars, and other observers of military matters:

> The internet has no shortage of photographs and videos showing armed men in Crimea who look like members of the Russian military. Their guns are the same as those used by the Russian army, their lorries have Russian number plates and they

> speak in Russian accents. Yet according to President Vladimir Putin, they are in fact members of "self-defense groups" organized by the locals who bought all their uniforms and hardware in a shop. This poses a challenge to the media covering the crisis: what do you call people who are officially not there? [22]

Just short of a year later, BBC News reported that Putin, in a documentary made for Russia's state-run news service, had admitted a military role in the annexation of Crimea well before Crimeans held a referendum on self-determination.[23] Certainly, Putin's moves in Crimea and the timing of his pronouncements suggest grand strategic design and operational planning.

Mathew Kroenig suggests that Russia, in knowing that it would likely fail in a direct conventional conflict with the United States and its North Atlantic Treaty Organization (NATO) allies, must "use hybrid warfare to make its revisionist actions as subtle as possible, avoiding moves that would trigger an automatic, robust response."[24] He describes the tools available to Russia via hybrid war thusly: (Russia) can use the pretext of protecting Russian nationals, ties to sympathetic elements within the victim country, propaganda campaigns, cyberattacks, irregular warfare including professorial soldiers in unmarked uniforms (the so-called little green men), and coercion through the massing of conventional forces on the border.[25] Kroenig and many others suggest that these were the tactics Russia employed in Georgia, eastern Ukraine, and Crimea. Further, creating and maintaining ambiguity is essential. Marcel Van Herpen, who has examined Russia's brand of hybrid warfare, writes:

> An integral part of this new kind of warfare is the "plausible deniability" of the implication of the aggressor nation's soldiers, Spetsnaz, or secret services. This "plausible deniability" is supported by an "information war" that accompanies the hostilities and that has the objective to convince public opinion at home and abroad of the aggressor's version of the facts.[26]

Contesting the cognitive domain through information warfare is a critical component of hybrid warfare. When an actor seemingly invests effort and resources into shaping public opinion for both domestic and foreign audiences it suggests it is attempting, at least to some extent, to avoid some undesirable outcome or cost. In other words, Russia's actions in Crimea imply that Russia's leadership was in some way uncertain or insecure about the possible backlash from foreign or domestic quarters. While that is likely true to some extent, by intentionally fostering the appearance of ambiguity Russia provided an escalation "off-ramp" for its adversaries. Ambiguity is useful to those playing for more time when the costs of direct intervention or further escalation seem too high.

While current analysis benefits from hindsight, the notional example attribution advantage model in figure 3 frames some of the attribution considerations for Russia's actions in Crimea. The specific values offered in this model and the others offered in this paper, though informed by available open-source information, are notionally assigned and intended to explore the terms and framework of the overall model (see appendix for more details on the author's scoring). That said, desired effect (*de*) and reciprocal vulnerability (*rv*), are notionally and subjectively rated here at 21 and 23 of 30 possible points. One cannot know whether Russian planners could have forecasted similar scores before the operation, but it seems feasible. Assuming the desired effect was a change in Crimea's political status, putting troops on the ground proved effective. Further, aside from possible reciprocal actions in cyberspace, Russia appears to have been relatively invulnerable to a Ukrainian response.

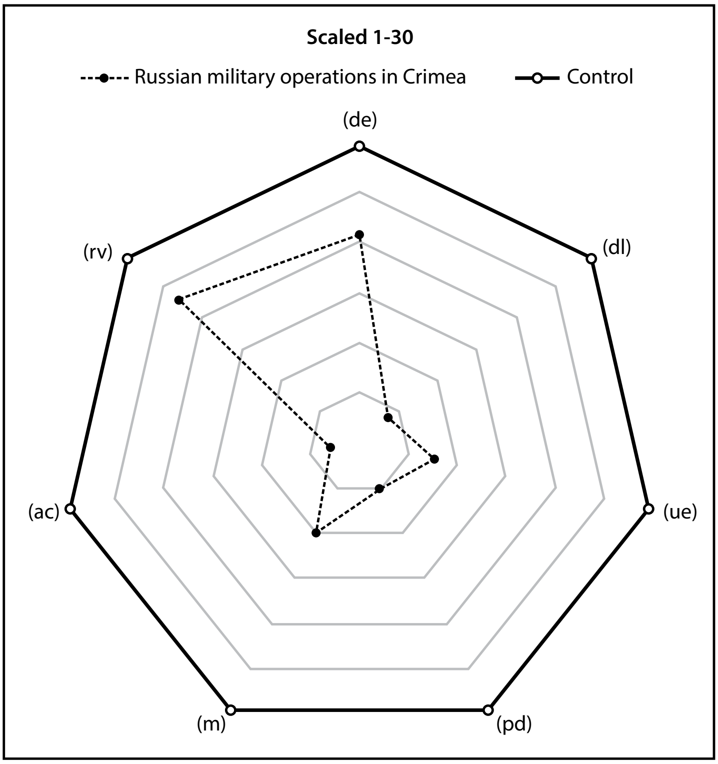


Figure 3. Attribution advantage in Crimea

However, as noted in the constriction in the curve, strategic and operational risk increases greatly across the remaining axes. Given the reasonable assessment that Ukraine would invest heavily to attribute an alleged violation of its sovereignty, the adversary's commitment (*ac*) moves close to center, a notional score of 3. The expected intense focus from both Western intelligence services and media coverage further suggest that misdirection (*m*) and plausible deniability (*pd*) values would also demonstrate high levels of operational risk, hence their notional scores of 5 and 10. Russia did reportedly experience unintended effects (*ue*) as a result of its overall operations in Crimea and Ukraine, and the score of 8 here that a planner might have forecasted may be generous. Perhaps the most notable example included the shoot-down of a Malaysian jet airliner, which resulted in 298 civilian deaths.[27] Despite Russian denials, numerous sources, including Ukraine, held Moscow responsible for the incident. Finally, given the situation on the ground, the success of misdirection (*m*) efforts seems to have been limited, despite Moscow's efforts to divert responsibility for the airline crash and other violations to other causes. Overall, this example model suggests that Russia's actions in Crimea were risky on a number of fronts and that ambiguity could never have been sustained for very long. However, given Russian forces' proximity to the operations area, Putin did not need much time. Whether Putin's opponents leveraged attribution problems and the appearance of ambiguity as a political cover for doing relatively nothing over that short span of time is another question.

Attribution Advantage in Practice: The Soviet Invasion of Afghanistan

The United States has frequently leveraged attribution to conduct covert operations. America's support to the Afghan mujahideen following the Soviet Union's invasion of Afghanistan remains one of the largest known covert operations in history, and it provides a useful example of weaponized attribution. In George Crile's account of the Central Intelligence Agency's (CIA) support to the mujahideen, plausible deniability seems to underlie every major decision. Crile describes how Charlie Wilson, a congressman from Texas, played a major role in helping, and sometimes forcing, the CIA to leverage the United States Congress's power of the purse to provide the mujahideen with the weapons they needed to fight the Soviet occupation. Plausible deniability was a constant necessity.[28] Crile states there was an "implicit understanding in Afghanistan" that the

"United States would not taunt the Soviets with an overt demonstration of involvement."[29] Policy makers and intelligence analysts determined that maintaining plausible deniability was necessary because they feared that in its absence, the conflict might escalate beyond the borders of Afghanistan.

Both Crile and Treverton make it clear that Pakistan's fear of a Soviet invasion drove the need for subterfuge.[30] Pakistan's leaders walked a tightrope amidst a backdrop that has become all too familiar. Refugees were pouring out of Afghanistan; creating the conditions necessary for their return meant aiding them in their fight against the Soviets. However, if those aid efforts went too far, the Soviets might retaliate. Pakistan's president frequently told foreign diplomats and military personnel "we must make the pot boil for the Russians but not so much that it boils over into Pakistan."[31] Facing a perennial threat from India, Pakistan could ill afford a second front with the Soviets.

The attribution advantage model helps explain attribution's role in the shifting nature of the risks the Americans and Pakistanis faced over time. Crile's account makes it clear that the Soviets enjoyed an asymmetric advantage over the mujahideen in the form of the Mi-24 "Hind" attack helicopter. The Hind was an armed killer, and the mujahideen stood little to no chance of success when a Hind appeared over battlefield. The question of what to do to help the mujahideen against the helicopters consumed Wilson and others. According to Crile, the CIA worked to ensure that any weapons provided to the mujahideen would appear as Soviet in origin.[32] The answer to the Hind problem lay in providing the mujahideen with a portable surface-to-air missile that could shoot down the helicopters. Crile writes that as late as the fall of 1985 those familiar with the problem knew the Stinger "was the best mule-portable plane killer in the world…but…the CIA was adamant about not introducing the American weapon. Putting in the Stinger would have been like advertising the CIA's involvement in the war in Red Square."[33] However, after a policy review, and facing the realization that plausible deniability was all but untenable given that "over three quarters of a billion dollars annually" was then flowing to the mujahideen, the CIA relented and the Stinger entered the fight.[34] The Stinger decision provides a benchmark for studying how the role of plausible deniability and attribution evolved over time.

The example model in figure 4 depicts the risks involved for the United States and Pakistan both prior to and after the introduction of the Stinger. By all accounts the Stinger made a significant impact in favor of the mujahideen. As the CIA understood, Russian detection rose and plausible deniability evaporated with the Stinger's arrival, hence the significant difference in their scoring. Unintended effects were a matter of great concern, and notionally score low in both scenarios at 10 pre-Stinger and 4 after. Crile writes that prior to 1986 "the idea of a Khomeini loyalist shooting down a TWA flight with a General Dynamics Stinger was too much" given the difficulty of controlling whose hands the missiles ended up in.[35] That concern suggests a higher than preferred level of reciprocal vulnerability (notional scores of 23 and 7). That the Soviets would dedicate significant resources to understanding the origin of the new threat killing its helicopters was a given.

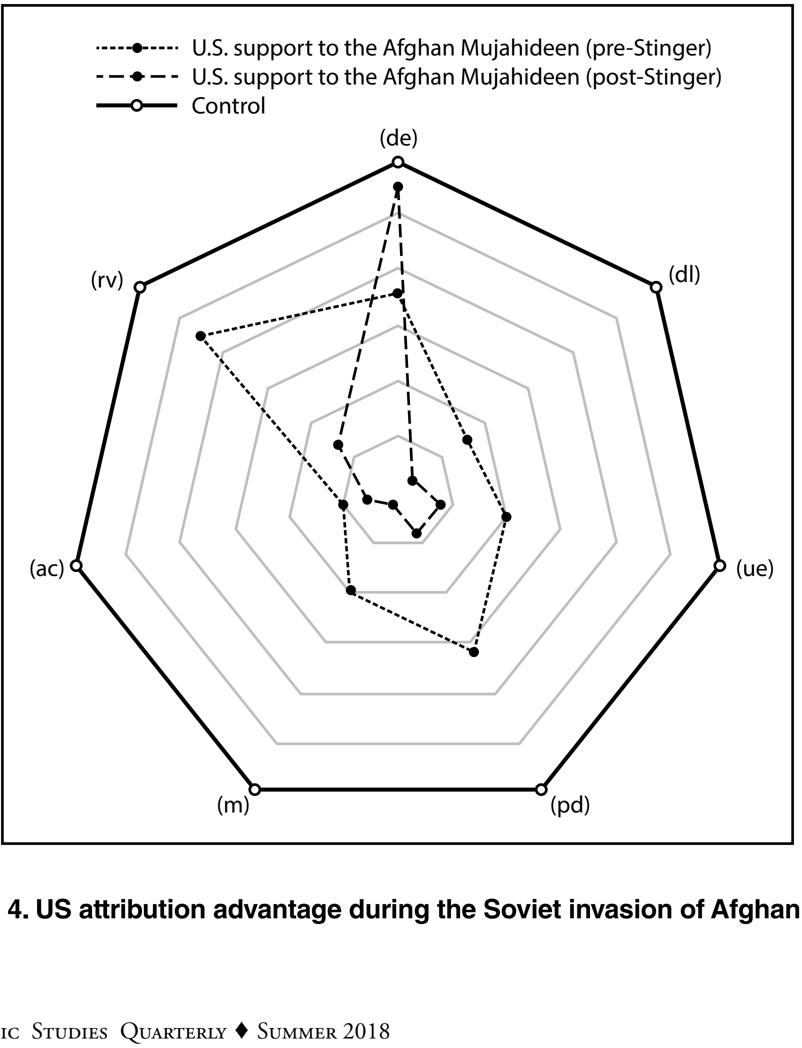


Figure 4. US attribution advantage during the Soviet invasion of Afghanistan

With hindsight emerges an additional unintended consequence, perhaps unfathomable to decision makers at the time. To maintain plausible deniability, American military aid to the mujahideen flowed through Pakistan. Crile contends that the Afghans "had no idea" their mules were loaded down with weapons paid for by American taxpayers, suggesting that to them, the weapons were "gifts from Allah" or perhaps Pakistan.[36] In his epilogue, Crile reflects deeply on the chain of events that connect the Soviet withdrawal from Afghanistan to the 11 September 2001 terrorist attacks. Crile does not frame the point explicitly, but one is left to wonder what impact a different approach to attribution taken early in the conflict might have had across the years that followed.

This example clearly reflects that time was an important factor in the context of the CIA's covert support. Early on the CIA planners wanted to raise the costs for Russia for as long as they could. They were unsure how long their mujahideen proxies could stand up to Russia's superior firepower. Once the Afghans proved their resilience the CIA's support grew to the point where attribution became more likely. That increased risk is evident in the model given how the points collapse in toward the center. However, by the time the Stingers were introduced to the battle space, the risk of Russian retaliation against Pakistan had become less of a concern.

Attribution Advantage in Practice: North Korea Goes Offline

December 2014 should be remembered as an important moment in the history of cyberwarfare. Controversy arose over a movie, whose unlikely plot revolved around a CIA attempt to assassinate North Korean dictator Kim Jong-un. The North Koreans were not amused. According to the BBC, as early as June 2014 a spokesman on North Korea's state-run news agency declared, "Making and releasing a movie on a plot to hurt our top-level leadership is the most blatant act of terrorism and war and will absolutely not be tolerated. . . . If the US administration allows and defends the showing of the film, a merciless counter-measure will be taken."[37]

Press reports from North Korea often seem rather hyperbolic and bellicose when focused on the United States. However, by the following November, Sony Pictures, the company responsible for *The Interview*, found itself to be the target of a crippling cyberattack. Sony's networks experienced severe outages, the salaries and social security numbers for thousands of employees were made public, and several unreleased movies leaked to the public.

North Korea publicly supported the hack but denied a direct role, suggesting that North Korean "supporters" and "sympathizers" around the world were likely responsible.[38] The saga did not stop there, even as Sony delayed release of the movie over terror threats to movie theaters. In mid-December, following Sony's delayed release, Kim Zetter, an internet security reporter for Wired.com, wrote:

> In the service of unraveling the attribution mess, we examined the known evidence for and against North Korea . . . . We have to say that attribution in breaches is difficult. Assertions about who is behind any attack should be treated with a hefty dose of skepticism. Skilled hackers use proxy machines and false IP addresses to cover their tracks or plant false clues inside their malware to throw investigators off their trail. When hackers are identified and apprehended, it's generally because they've made mistakes or because a cohort got arrested and turned informant.[39]

Given the stated difficulties of cyber attribution, Zetter and her team at Wired.com concluded that the available evidence against North Korea was thin and circumstantial.[40] Of note, two years later Fred Kaplan stated in his book *Dark Territory: The Secret History of Cyber War* that the National Security Agency "had long ago penetrated North Korea's networks: anything that its hackers did, the NSA could follow."[41] Still, the entire episode frames the difficult issue of cyber attribution—but the story does not end there.

Just days after Zetter's analysis in Wired.com, someone or something severed North Korea's extremely limited connection to the internet.[42] According to Kaplan and his sources:

> The United States government played no part in the shutdown. A debate broke out in the White House over whether to deny the charge publicly. Some argued that it might be good to clarify what a proportional response was not. Others argued that making any statement would set an awkward precedent: if U.S. officials issued a denial now, then they'd also have to issue a denial the next time a digital calamity occurred during a confrontation; otherwise everyone would infer that America did launch that attack, whether or not it actually had, at which point the victim might fire back.[43]

It is worth noting that at least one group reported evidence and published analysis suggesting that North Korea's loss of its internet connectivity was due to a distributed denial of service attack and that a hacktivist group was likely involved.[44] Still, the dilemma for US policy makers in similar situations remains. Time is a valuable commodity in a place like Washington, DC, where the next election, congressional recess, or holiday is always looming. Time spent debating a response to accusations is time not spent advancing other agendas. Thus, in the cyber domain, when someone else seizes attribution advantage, the effect on decision cycles in terms of debating response options is very real.

As in the earlier scenarios, the attribution advantage model (see figure 5) is intended to help planners and decision makers ask good questions about these respective operations. The assessments represented by the graph are intended as examples, though they are somewhat informed through the benefit of hindsight and open-source information. At the very least, those capable of carrying out operations such as these should be able to make an assessment in response to the questions posed in the model. Of note, the following analysis assumes that someone intentionally took down North Korea's internet, meaning human or mechanical error was not to blame, although that still remains possible.

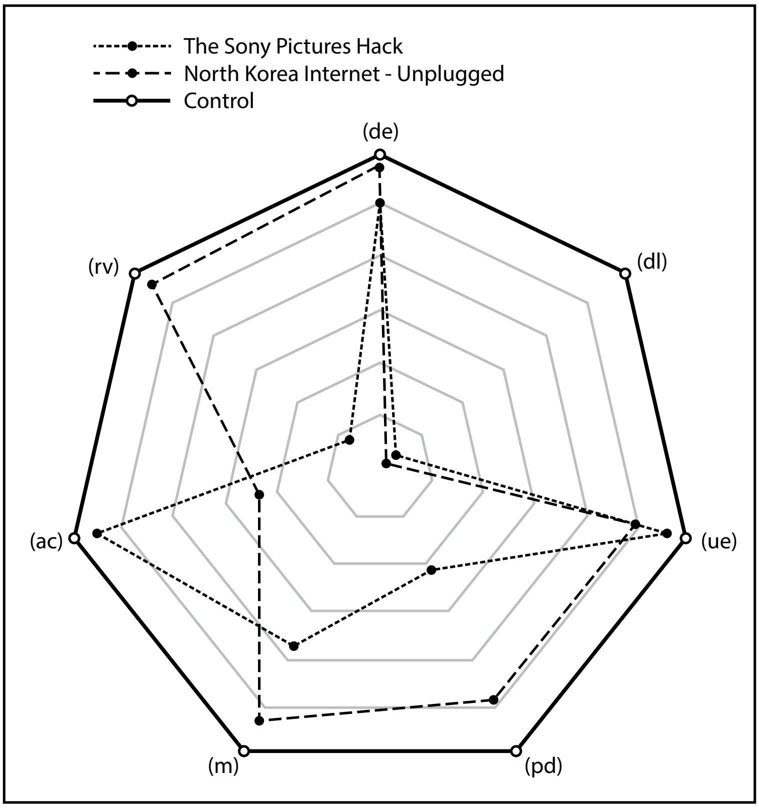


Figure 5. North Korea cyberwarfare, 2014

Clearly both attacks should score highly in terms of desired effect. This model assesses their notional score at 28 and 30 on the 30-point scale. North Korea's internet infrastructure, by all accounts, is made vulnerable by its small scale. While the Sony Pictures hack proved highly effective, in both cases the perpetrators likely had a reasonable expectation that they could achieve their desired effects. Of course, the perpetrators should not have had any expectation of their attack going undetected given the nature of the attacks. The model assesses a detection likelihood score of close to zero. These attacks were fundamentally different than other famous attacks. Stuxnet, the cyberattack against Iran's uranium centrifuges, likely provides a better example of an attack in which stealth was pursued. In fact, stealth was central to the worm's trust-exploiting design. Of Stuxnet, cyber experts Singer and Friedman write, "the most insidious part [is] . . . it was an integrity attack par excellence. Stuxnet didn't just corrupt the process, it hid its effects from the operators and exploited their trust that the computer systems would accurately and honestly describe what was taking place."[45]

Stealth, in terms of the target not knowing anything was happening, was not a requirement in the Sony hack or the attack that severed North Korea's internet. When Sony's users logged onto their machines in the early stages of the attack they were greeted by skulls on their monitor accompanied by a message that they had been hacked.[46] One can assume Kim Jong-un quickly discovered that his internet connection had been severed. Stuxnet provides a good example of an effect created to put more time on the clock for other political actions.

Unintended effects are more difficult to judge in this case based on the available open-source information, but logic suggests the chances of unintended effects were low, notionally scoring 26 for the Sony hack and 23 for North Korea going unplugged. If the assailants that severed North Korea's internet connection had only intended to bring down one website, for example Korea's state-run news agency, then they overreached in their attack. This seems unlikely given the aforementioned evidence that a denial of service attack brought down North Korea's internet. The "smash and grab" nature of the Sony hack leaves little room for consideration of unintended effects.

Plausible deniability and misdirection seemingly discover high scores on the graph. The model in figure 5 rates their possible values at 25 and 19 respectively. Kaplan attributed the Sony hack to North Korea, but only with the apparent hindsight benefit of a source that may have had access to classified US government information. Attribution seemed far less certain for Zetter at Wired.com and others. While circumstances led many to assume the United States turned off North Korea's internet, Kaplan is equally decisive in his claim that the United States was not responsible. It is difficult to know if the respective assailants concerned themselves much with attribution or misdirection. That said, their results speak for themselves.

For the hackers who conducted the attacks, judging their adversary's commitment to attribution and their own reciprocal vulnerability seems relatively straightforward. Surely Sony's assailants understood that Sony, a leading institution in a multibillion dollar industry, could marshal significant resources for attribution on its own, not counting any support that might have been offered by the US government. Indeed, without help from China or some other interested party, North Korea would seem to have fewer capabilities available for attribution than Sony. The model assesses a high score for reciprocal or "in-kind" vulnerability for whoever cut North Korea's internet, as North Korea seems to have been unable to appropriately place the blame. As such, for North Korea, whether the attacker was a hacktivist group or cyber warriors based in the United States, returning the favor would likely have proven difficult.

Again, for the purposes of this analysis the question of reciprocal vulnerability focuses on whether an attacker should fear their cyber weapon being turned on them. In other words, if an attacker "unveils" a new weapon in any domain then reciprocal vulnerability should be a concern. Whoever attacked Sony likely had only minor concerns in this area. Surely they would have assumed that Sony would not respond directly. A better question might have been whether or how the United States would respond. One might surmise from Kaplan, or from Singer and Friedman's depiction of the various policy debates, that America would not have responded to an attack against a business with an all-out cyber assault of its own.

This leaves hacktivist groups, which represent something of a wild card. Hacktivists militantly support a variety of issues, so the potential for a reciprocal attack conducted as retribution for the Sony hack seems high. For example, the loose-knit hacker group known as Anonymous has a reputation for retaliating against the suppression of speech. Hacktivists emerge as likely suspects in the attack that led to North Korea briefly losing its internet connection. Indeed, when thinking about reciprocal vulnerability, the question of who will respond to an attack, if the attack is properly attributed, seems just as important as whether someone will reciprocate. Some actors are simply far less constrained than others.

Recommendations for the Future

Accept Risks at Lower Command Echelons

US Army doctrine defines operational art as "the pursuit of strategic objectives, in whole or in part, through the arrangement of tactical actions in time, space, and purpose."[47] That definition appropriately conveys the requirement for military planners to synchronize operations across war-fighting domains. There simply is no potential for synchronicity and synergy if the right effects do not happen across the desired domains at the right time. Therefore, if a nonattributed effect is desired, that effect must be generated at the right moment in concert with other more visible efforts.

Further, in line with deception doctrine, there must be an operational reason to pursue nonattribution. One area where nonattributed effects might prove particularly effective is in shaping the battlespace in support of future operations. Kaplan relates the story of Operation Orchard, in which he claims that an elite Israeli cyber unit successfully hacked Syria's air-defense radars in such a way as to keep Syria's radar screens blank while the Israeli Air Force launched a devastating attack on a Syrian nuclear facility.[48] To maximize the chance that their fighters could penetrate Syrian airspace unnoticed, the Israeli team had to achieve the cyber effect at just the right time. This was a covert cyber operation, a perfect example of a covert, nonattributed effect achieved at just the right time, for just the right amount of time, in support of the overall operational plan.

The Operation Orchard example highlights the necessity for synchronization across domains or, put another way, it is an example of multi-domain operations in action. That level of integration and planning suggests several things about planning and execution. Clearly, an airstrike against another country's secret nuclear program would require strategic level direction. However, planning, coordination, and execution in real time could likely have occurred at a lower echelon. Indeed, given the synchronization necessary for the cyber operators to control the Syrian air picture just as the fighters were preparing to penetrate Syrian airspace suggests the necessity for tight command and control integration. It also implies that the Israelis were prepared to "lose" whatever tool they employed in the hack. That willingness is critical for synchronizing operations at lower echelons.

This suggests the need for further development of operational constructs and doctrine that push planning, decision making, and execution for non-attributable effects down to lower command echelons. The establishment of small teams at multi-domain operations centers (MDOC) with access to US Cyber Command tools and authorities that resemble Air Force National Tactical Integration cells that already support the air component in the joint fight seems warranted. These specially trained, cyber-oriented integration teams would play a key role in helping future MDOC strategy and targeting cells leverage attribution as a source of advantage.

The attribution advantage model examples seem to support the idea of pushing execution authority for nonattributed effects to lower echelons. In near perfect conditions of attribution supremacy, the overall risk is such that decisions impacting real-time coordination and execution can likely be assigned to lower echelons of command. Of course, the highest echelon authority would most likely always need to approve something like Operation Orchard. The Israelis appear to have intended that operation as a surgical use of military force, in what was likely hoped to be a singular event. However, had the Israeli action been part of a prolonged air campaign, the operation might better have been served by pushing authorities down and accepting risk at lower echelons. Pushing that risk down to lower echelons with necessary authorities and capabilities should be considered because doing so seemingly creates opportunities to begin winning the conflict to the left of "Phase 0" on traditional planning timelines.

Self-Attribute to Win Time and Boost Deterrence

Attribution challenges traditional thinking about deterrence, and formulating deterrence strategies against adversaries that have achieved attribution advantage seems inherently difficult. This is because deterrence begins with one actor understanding the capabilities and actions of another. There is an inherent promise within deterrence that some form of costly retaliation will occur if one actor crosses the "red line" of another. Such retaliation begins with realization and attribution. If one is unaware of being attacked or is unable to attribute the attack, effective retaliation is difficult. In this way, nonattribution creates a difficult problem for effective deterrence strategies. However, self-attribution, which involves credibly claiming responsibility for an act one may or may not have committed, emerges as a tool that can help commanders influence the timing and tempo of conflict.

John Norton Moore brilliantly explored the role deterrence plays in conflicts outside the digital realm between democracies and non-democracies. He defined "effective deterrence" as the "aggregate of external incentives known to and understood by a potential aggressor as adequate to prevent the aggression."[49] A critical aspect of the relationship between deterrence and attribution is that an actor with digital realm attribution advantage can add two critically important words to the end of Moore's definition: "if caught." Further, in his 2003 essay entitled "Solving the War Puzzle," Moore reached an important conclusion. While exploring the dynamic between democracies and non-democratic states engaged in war he found that "the principle path to major interstate war for democracies seems to be failing to ensure adequate levels of deterrence when confronted by potential aggressors."[50] Moore then summarized the reasons why deterrence fails:

> Deterrence failure can occur because of an absence of adequate military forces, as was true of the U.S. entry into World War II and, in part, the Japanese attack on Pearl Harbor; lack of communication of intent (or even any advance formation of an intent to defend), as was true in the Korean and Gulf Wars; or lack of believability of the guarantee, as was true of British entry into World War II and, in part, Milosevic's decisions to defy NATO in Bosnia and Kosovo.[51]

Moore focused on interactions between nations, but his conclusions about deterrence would better hold up against a range of state and nonstate actors were it not for the complications created by the difficulty of attribution in the cyber domain. Attribution creates an obstacle for deterrence and incentivizes attacks by the weak against the strong.

Henry Kissinger senses the danger in the difficulties of cyberattack attribution. In *World Order*, Kissinger writes that "internet technology has outstripped strategy or doctrine—at least for the time being."[52] What he means is that the combination of the public's reliance on the internet and the internet's current and perhaps inherent vulnerabilities creates incongruence within the international system. Attribution is at the core of his concerns as Kissinger asserts that "when individuals of ambiguous affiliation are capable of undertaking actions of increasing ambition and intrusiveness, the very definition of state authority may turn ambiguous."[53] He continues, stating "actions undertaken in the virtual, networked world are capable of generating pressures for countermeasures in physical reality, especially when they have the potential to inflict damage previously associated with armed attack."[54] But how certain must a "responsible" actor be of the culprit after a particularly damaging or disruptive attack? Such is the nature of attribution advantage.

A nation under cyberattack may feel pressured from within to retaliate, but uncertainty about who conducted the attack and why can lead to decision paralysis or, perhaps worse, conflict escalation with a rival that may not even be responsible for the attack. In a broader sense, time can be thought of as an output in deterrence-based equations. The United States and the Soviet Union seemed destined for armed conflict for decades during the Cold War. However, during moments of crisis the existence of nuclear weapons provided a deterrent to conflict escalation. This bought both sides the time necessary to attempt to achieve their political goals through less destructive means, at least until one side exhausted the resources necessary to sustain the status quo.

The difficulty of the attribution problem and whether attribution remains beyond the reach of traditional deterrence strategies is up for debate. Kissinger suggests that this "new world of deterrence theory and strategic doctrine now in its infancy requires urgent elaboration."[55] USAF Gen Kevin Chilton, in line with Moore's analysis of deterrence failure, suggests that part of the problem is "the lack of a known historical track record of US detection, attribution, and response" which fundamentally challenges the credibility of deterrent threats.[56] He further advocated that responses to cyberattacks need not be limited to the cyber domain.[57] Therein lies the key. If one accepts the notion that time is an output of deterrence calculus, then self-attribution seemingly becomes necessary. If deterrence is a function of capability, credibility, and communication, then at some point capabilities must be made known.

Lindsay points out attackers may derive some benefit in terms of acknowledged capability once an effect for which they are responsible is attributed.[58] Doing so certainly requires the type of thorough evaluation explored above. In the cyber realm, transparency probably means that some techniques, tools, and even networks should be set aside from more elegant capabilities and made visible only if doing so supports the commander's intent. If a status quo develops in which no one admits capabilities, no one admits detecting the capabilities of others, and no one risks responding to cyberattacks for fear of revealing detection methods, then the ability of deterrence to serve as a well from which to draw time will remain diminished.

Wargame Attribution Advantage

Unlocking the full potential inherent in the above recommendations for weaponizing attribution requires investment in two enabling concepts. First, multi-domain attribution choices must be present in operational war gaming and exercises. Helmuth von Moltke the Elder, who in his military career mastered sweeping technological advances in firepower, transportation, and logistics technology, wrote, "We in the military pay due attention to the progress of science and to inventions in other than military matters. But an invention is not what it is in itself. The value of any invention rests not only in theory, even if correct, but mainly on its practical application by complete technical development . . . it will therefore no longer suffice merely to observe what is done in other areas. We must ourselves perfect the invention."[59]

Perfecting inventions and mastering operational concepts requires realistic training, exercises, and war gaming. A report published by the Defense Science Board echoes Moltke's comments: "Effective experiments are an innovation-enabler . . . these procedures can improve the effectiveness of new defense systems and can create surprise, challenge our adversaries, and help anticipate how new technologies and systems concepts might be used against U.S. forces."[60]

Personalized training tailored to every echelon of command across scenarios modified to present different challenges has the potential to make training more realistic than ever.

Gaming technology and virtual reality will have the potential to increase the frequency and lower the cost of training. While there is nothing that quite compares to the danger of being under fire, technology is creating the opportunity for training opportunities that are profound in their realism. Soldiers, Sailors, Marines, and Airmen must be allowed to employ techniques and tools that leverage the underlying premise of attribution advantage. For example, cyber domain war games must accurately demonstrate how accesses gained and maintained months or even years before what one might consider the traditional beginning of Phase 0 shaping operations can be brought to bear and synchronized with other effects.

Of course, training should not just revolve around using cyber and other tools to leverage attribution advantage. Commanders at all levels should consider how to respond and even how best to render their best military advice, when the adversary has seized attribution advantage for itself. How does one structure one's thinking in formulating a response when the assailant's identity and motivations are ambiguous? In his book *Misguided Weapons,* Israeli defense expert Azriel Lorber describes a type of technological surprise in war whereby the "existence of a new weapon is known," but its capabilities are not fully considered across "potential battlefield scenarios."[61] Lorber also describes situations where an adversary had actually faced a weapon before, but for whatever reason—perhaps because lessons were not properly learned and applied—is surprised more than once by the same technology. He call this unfortunate state "self-inflicted surprise."[62] Unless war fighters are allowed to succeed and fail in their efforts to leverage attribution advantage it is difficult to imagine how the potential of those techniques might be fully realized in war. Further, war fighters who have not been trained to adequately anticipate and respond to the attribution problems posed by adversaries would seem to be at a disadvantage here, in what may prove to be the age of hybrid warfare.

Defend with Open-Source Intelligence

A second enabling concept required for achieving attribution advantage involves placing increased focus on and investment in open-source intelligence collection, processing, and analysis. Attribution advantage cannot be thought of in offensive terms only. Attribution superiority involves achieving attribution advantage in support of one's own operations while denying it to the enemy. Therefore, defensive measures must be anticipated to thwart the efforts of adversaries who might weaponize attribution toward their own ends.

Open-source intelligence and data mining seem to hold some promise in this regard. Looming advances in artificial intelligence (AI) systems meant to improve our personal lives will quickly find military applications.

AI-empowered analytical processes may prove to be incredibly powerful for open-source intelligence. In his book *The Inevitable*, Kevin Kelly writes about how Google Photo's AI can remember objects in every one of the 130,000 pictures he has uploaded. He also points out that Facebook has AI capable of correctly identifying a single person's face in a crowd of billions.[63] What if that same computer vision technology had been employed against Putin's little green men? In scenarios like Crimea, political leaders may not be able to counter the claims of their rivals without exposing sensitive sources and methods. Open-source intelligence enhanced by artificial intelligence and machine learning seems both promising and necessary.

If one considers open-source intelligence as encompassing everything from foreign news services to tourists posting pictures on social media, what begins to emerge is a data-rich, yet chaotic, information environment. Col Jason Brown recently described this potential as "seeing the data trails" left behind by the various actors in a conflict and described how a "simple tweet" sent at the wrong time could have "blown the cover of the SEAL team sent to kill Osama bin Laden."[64] The varying degree of chaos in the data trails will make following those trails difficult for humans acting alone. This is because the raw data is created and moves throughout the environment in myriad ways.

For example, a tornado forms near a city. The local news channels will report on the event, weather radars will provide data, and individuals near the affected area will take pictures before, during, and after the event. Eventually a complete picture of the event, informed by numerous sensors, emerges and enhances understanding of what happened. AI systems have the potential to bring order out of that chaotic information environment, creating decision-quality information in less time than humans could ever manage on their own. This holds tremendous potential in making weaponized attribution both an offensive and a defensive reality. When an actor in the conflict claims not to be responsible for some atrocity that has happened, AI-driven systems may eventually be able to provide analysts with the open-source information necessary to refute that claim. Disinformation from "fake news" will find itself surrounded by "antibodies" of truth at machine speed. This means the side that better exploits emerging AI technologies will hold a clear advantage in the contest for time. They will be capable of sense-making faster than their adversaries and will be able to burn through the false narratives future adversaries push in the information environment in less time. From that come flexibility and increased decision space.

Conclusion

Time is everything in attribution advantage. Decision cycles turn upon the ability of command and control systems to accurately connect actions with actors. Attribution emerges as a fundamental component throughout decision making. The problems that attribution can create present both an opportunity for fresh thinking about targeting and a challenge in terms of deterrence, defense, and retaliation.

A number of topics addressed in this article would benefit from additional research. The models captured in the spider graphs were provided as examples intended to help facilitate analysis of the model itself and how the attribution advantage model presented here might help decision makers and planners visualize the risk and opportunities inherent to the pursuit of nonattributed effects. The notional values assigned to the model's various components were derived from unclassified open-source material. While classified data would better inform real-world model employment, for the purpose of this paper the exact numeric values depicted are meant to explore the terms of the model and the general phenomenon of attribution. The real question is whether the attribution advantage model would aid strategic decision makers, commanders, and operational planners with questions about whether to employ nonattributed effects prior to conflict. Exploring that requires specifically tailored war gaming. Finally, the costs and implications of the recommendations made in this paper need further refinement and exploration at a higher classification.

The question of attribution seems to turn upon the degree to which one is seeking to either foster uncertainty or produce friction in adversary systems. There are many scenarios where maintaining the stealth of the effects being generated for as long as possible is necessary to generate the maximum amount of friction in the adversary's systems. Yet, one should expect and plan for every covert operation to be discovered eventually. Still, therein opportunities to gain further advantage await. Leveraging the moment when an adversary discovers a previously undetected effect to foster uncertainty about the effect's origin will often cause the adversary to expand their decision cycles as they attempt to decipher what is happening and who to blame. However, self-attribution, conducted aggressively and defiantly at the proper moment, may cause the adversary to question the reliability of other data streams. Self-attribution, if accomplished without compromising exquisite, irreplaceable tools and capabilities, seems necessary for reinforcing deterrence, especially in cyberspace.

Seizing attribution advantage means controlling or influencing what adversaries know about what is happening to them, and most importantly, who they blame. This provides the operational artist with a unique method of influencing or even dictating the timing and pace of events, even as they produce additional effects across multiple domains. Therefore, attribution should be made more explicit in planning multi-domain operations, especially for the early phases of conflict. While no one can alter the physics of time, military planners and targeteers should seek to influence the pace at which events unfold. Planners can guide their adversaries toward hasty decisions made on faulty premises or even generate and later take credit for effects that cause adversaries to have so little trust in their data streams that it paralyzes their decision making. There is great opportunity for those who seek and seize the initiative in such moments.

APPENDIX
Author's Note on Scoring with the Attribution Advantage Model

As described in the text, scoring within the attribution advantage model is necessarily subjective in that it will always be based on imperfect all-source knowledge of the adversary and, potentially, imperfect knowledge of one's own capabilities. Still, decision makers and planners need ways to structure their thinking about how to identify those moments prior to or even during a conflict when they might hold attribution advantage. Further, the attribution advantage model provides a visualization of risk. The more points an analyst plots toward the center, the higher the assessed level of risk.

Whether employed academically or as an operational planning tool, the scores within the model can only be assessments made from the best available information. For example, operational planners might assess that there is zero percent chance that an effect will have unintended consequences during or after execution. Utilizing this model, they would give *ue* a score of 30. The planners would then be wise to have an explanation for their certainty ready prior to briefing their commander, because any commander well trained or tested by the inherent uncertainties of war will challenge that assessment. This model is presented as a tool intended to structure both the commander's and the planners' thinking while providing a visual aid that highlights the risks involved in generating effects that one would prefer to remain unattributed, either forever or until the moment of their choosing.

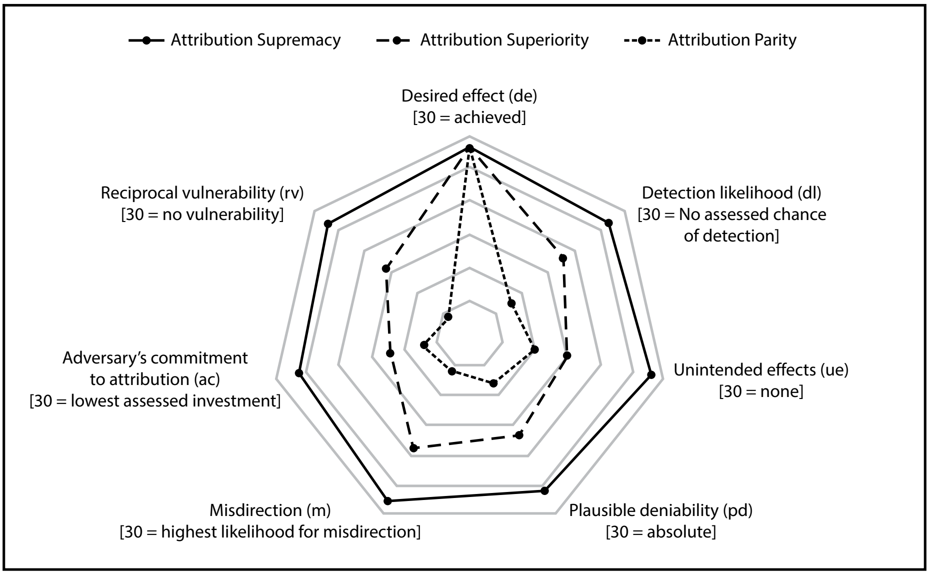
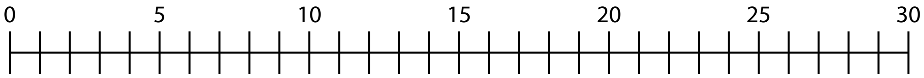


Figure 6. The attribution advantage model

The following scales are offered to further explain the author's intent for scoring in the model, to illustrate scoring in the mini-case studies, and to guide others who might use the model.

Desired Effect

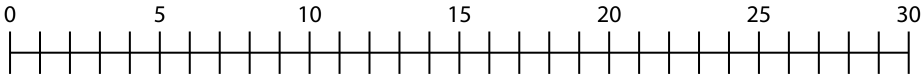


0: No assessed chance of achieving desired effect with the capability in question. This might be due to hardening or redundancy in the target or the nature of the adversary's political system.

15: The odds of achieving the effect are assessed at 50 percent given the nature of the target, the adversary's preparations for the intended effect, and the nature of aggressor capabilities.

30: Achieving the desired effect is an absolute certainty given a clear overmatch between the aggressor's available capabilities and the adversary's vulnerabilities.

Detection Likelihood

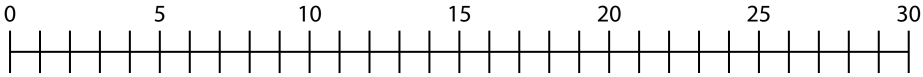


0: The adversary will detect or notice this effect the moment it is generated.

15: The odds of detection are assessed at 50 percent given the nature of the adversary, the adversary's defenses, and the nature of tools available to achieve the effect

30: There is no chance the adversary, or any other party, will ever detect the planned effect.

Unintended Effects

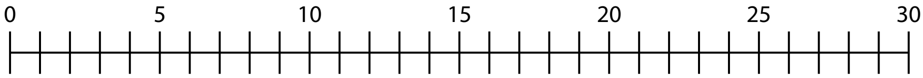


0: The effect, once employed, will spread in ways the aggressor cannot control and will have numerous unintended effects throughout the targeted system.

15: The likelihood of unintended effects generated is 50 percent, due to limited testing, lack of knowledge about the offensive capability, and unknowns in the targeted system.

30: There is no chance of unintended effects based on superior understanding of the target system and a high degree of successful operational testing of the capability being considered.

Plausible Deniability

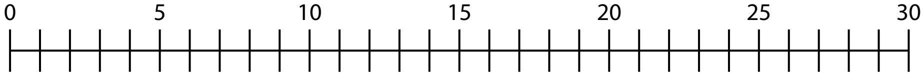


0: There is zero chance that the aggressor can make the targeted party and the rest of the world think that some other party is responsible for this effect.

15: The odds that the aggressor can plausibly deny responsibility for the generated effect are 50 percent, given the adversary's defenses, third-party interest, and the nature of available capabilities required to achieve the effect.

30: There will never be enough proof for an adversary or third party to positively attribute the effect to the aggressor with the certainty necessary to justify retaliation.

Misdirection

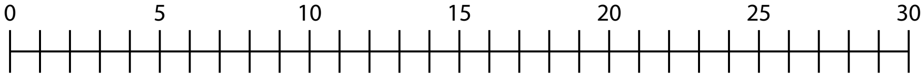


0: Not only will the aggressor's action be detected, but also any steps the aggressor took to make it look like some other party was responsible will also be noticed.

15: The odds of misdirection working are assessed at 50 percent given the nature of the adversary, the adversary's defenses, and third-party interest and investigation.

30: The aggressor's efforts to cause its adversary to believe that some other party is to blame for the aggressor's actions succeed with absolute certainty given the technology in play or the adversary's predispositions and impatience with forensic efforts.

Adversary's Commitment to Attribution

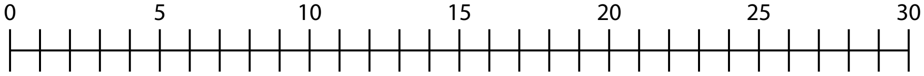


0: The adversary and interested third parties possess limitless resources and commitment to forensic efforts designed to uncover the party responsible for the generated effect.

15: The adversary and aligned third parties can bring significant forensics capability to bear, and odds that they will eventually attribute an effect accurately are assessed at 50 percent.

30: The adversary completely lacks forensics capability with the aggressor's vector for covert attack, and third parties are either unaware or uninterested in offering outside assistance.

Reciprocal Vulnerability



0: The aggressor shares the same vulnerabilities as the adversary, and if the capability is employed, the aggressor will inevitably and unavoidably fall victim to the same capability.

15: The odds of the aggressor finding itself vulnerable to the effects it intends to generate against an adversary are 50 percent, given incomplete efforts to insulate itself from the capability.

30: The aggressor's capabilities are so tailored and precise, and its own defenses are so secure, that the aggressor is completely immune from the capabilities it intends to unleash against its adversary's in pursuit of some desired effect.

Notes

[1] Gen David Goldfein, "Remarks to 2016 Air Force Association Air, Space, and Cyber Conference" (speech, National Harbor Maryland, 20 September 2016), http://www.af.mil/Portals/1/documents/csaf/Goldfein_Air_Force_Update_Sept_2016.pdf.

[2] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1-2 (2015): 4–37, http://doi.org/ckvx.

[3] John R. Boyd, *Patterns of Conflict* (presentation notes, December 1986), slide 7, http://www.danford.net/boyd/patterns.pdf, accessed 3 March 2017. For more on Boyd's concepts, see his new book *A Discourse on Winning and Losing* (Maxwell AFB, AL: Air University Press, 2018), http://www.airuniversity.af.mil/AUPress/Books/.

[4] Boyd, *Patterns*, slide 7.

[5] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1984), 117–18.

[6] Boyd, 102.

[7] Nicholas G. Carr, *The Shallows: What the Internet Is Doing to Our Brains* (New York: W. W. Norton, 2010), 131.

[8] Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2013), 20–22.

[9] Kahneman, *Thinking*, 85.

10. Kahneman, 85.

11. Department of Defense (DOD), Joint Publication (JP) 3-13.4, *Military Deception* (2017), I-1.

12. DOD, *JP 3-13.4*, I-4.

13. Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (June 2015): 316-348, http://dx.doi.org/10.1080/09636412.2015.1038188.

14. Roger T. Ames, *Sun Tzu, The Art of Warfare: The First English Translation Incorporating the Recently Discovered Yin-ch'üeh-shan Texts*, 1st ed. (New York: Ballantine Books, 1993), 104.

15. Boyd, *Patterns*, slide 41.

16. Boyd, slide 13.

17. Gregory F. Treverton, *Covert Action: The Limits of Intervention in the Postwar World* (New York: Basic Books, 1987), 4.

18. Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/17): 44–71, https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266.

19. Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack," *Journal of CyberSecurity* 12, no. 1 (September 2015): 4, https://doi.org/10.1093/cybsec/tyv003.

20. David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, 1st ed. (New York: Crown Publishers, 2012), 205.

21. Treverton, *Covert Action*, 4.

22. Vitaly Shevchenko, "'Little Green Men' or 'Russian Invaders?' " BBC News, 11 March 2014, http://www.bbc.com/news/world-europe-26532154.

23. "Putin Reveals Secrets of Russia's Crimea Takeover Plot," BBC News, 9 March 2015, http://www.bbc.com/news/world-europe-31796226.

24. Mathew Kroenig, "Facing Reality: Getting NATO Ready for a New Cold War," *Survival* 57, no. 1 (February–March 2015): 45, http://doi.org/bt9t.

25. Kroenig, "Facing Reality."

26. Marcel Van Herpen, *Putin's Wars: The Rise of Russia's New Imperialism*, 2nd ed. (London: Rowman and Littlefield, 2015), 270.

27. Nicola Clark and Andrew E. Kramer, "Malaysia Airlines Flight 17 Most Likely Hit by Russian-Made Missile, Inquiry Says," *New York Times*, 13 October 2015, https://www.nytimes.com/2015/10/14/world/europe/mh17-malaysia-airlines-dutch-report.html?_r=0.

28. George Crile, *Charlie Wilson's War: The Extraordinary Story of the Largest Covert Operation in History* (New York: Atlantic Monthly Press, 2003), 217–18.

29. Crile, *Charlie Wilson's War*, 217.

30. Treverton, *Covert Action,* 213.

31. Crile, *Charlie Wilson's War*, 128.

32. Crile, 105.

33. Crile, 405.

34. Crile, 419–21.

35. Crile, 405.

36. Crile, 105.

37. "North Korea Threatens War on US over Kim Jong-Un Movie," BBC News, http://www.bbc.com/news/world-asia-28014069, accessed 10 March 2017.

38. "North Korea Denies Responsibility for 'Righteous' Hack Attack on Sony," BBC News, http://www.bbc.com/news/world-asia-30366449, accessed 10 March 2017.

39. Kim Zetter, "The Evidence that North Korea Hacked Sony Is Flimsy," Wired.com, 17 December 2014, https://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin/.

40. Zetter, "Evidence."

41. Fred M. Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016), 269.

42. Nicole Perlroth and David E. Sanger, "North Korea Loses Its Link to the Internet," *New York Times*, 22 December 2014, https://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html?_r=0.

43. Kaplan, *Dark Territory,* 271–72.

44. Dan Holden, "North Korea Goes Offline," Arbor Networks, 22 December 2014, https://www.arbornetworks.com/blog/asert/north-korea-goes-offline.

45. P. W. Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, ed. Allan Friedman (New York: Oxford University Press, USA, 2014), 117.

46. "The Interview: A Guide to the Cyber Attack on Hollywood," BBC News, 29 December 2014, http://www.bbc.com/news/entertainment-arts-30512032.

47. US Army Doctrine Publication 3.0, *Unified Land Operations* (Washington, DC: Headquarters, Department of the Army, October 2011), 9, https://www.army.mil/e2/rv5_downloads/info/references/ADP_3-0_ULO_Oct_2011_APD.pdf.

48. Kaplan, *Dark Territory*, 160–61.

49. John Norton Moore, "Solving the War Puzzle," *American Journal of International Law* 97, no. 2 (April 2003): 285, http://www.jstor.org/stable/3100103.

50. Moore, "Solving," 286.

51. Moore, 286.

52. Henry Kissinger, *World Order* (New York: Penguin Press, 2014), 344–45.

53. Kissinger, 344–45.

54. Kissinger, 346.

55. Kissinger, 347.

56. Kevin Chilton and Greg Weaver, "Waging Deterrence in the Twenty-First Century," in *Proceedings: Deterrence in the Twenty-First Century*, ed. Anthony C. Cain (Maxwell AFB, Alabama: Air University Press, 2016), 72.

57. Chilton and Weaver, "Waging Deterrence."

58. Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack," *Journal of Cybersecurity* 1, no. 1 (September 2015): 3, https://doi.org/10.1093/cybsec/tyv003.

59. Helmuth Moltke and Daniel J. Hughes, *Moltke on the Art of War: Selected Writings* (Novato, CA: Presidio Press, 1993), 257.

60. Defense Science Board, "Technology and Innovation Enablers for Superiority in 2030" (Washington, DC: Defense Science Board, 2013), 78, http://www.dtic.mil/dtic/tr/fulltext/u2/a608507.pdf.

61. Azriel Lorber, *Misguided Weapons: Technological Failure and Surprise on the Battlefield* (Washington, DC: Brassey's Inc., 2002), 229–30.

62. Lorber, *Misguided Weapons*, 230.

63. Kevin Kelly, *The Inevitable: Understanding the 12 Technological Forces that Will Shape Our Future* (New York: Viking, 2016), 46.

64. Jason Brown, "In the Information Age: Centers of Activity > Centers of Gravity," *Medium*, 5 May 2015, https://medium.com/@jasonmbro/in-the-information-age-c70622a61bc9.

Disclaimer

The views and opinions expressed or implied in SSQ are those of the authors and are not officially sanctioned by any agency or department of the US government. We encourage you to send comments to: strategicstudiesquarterly@us.af.mil