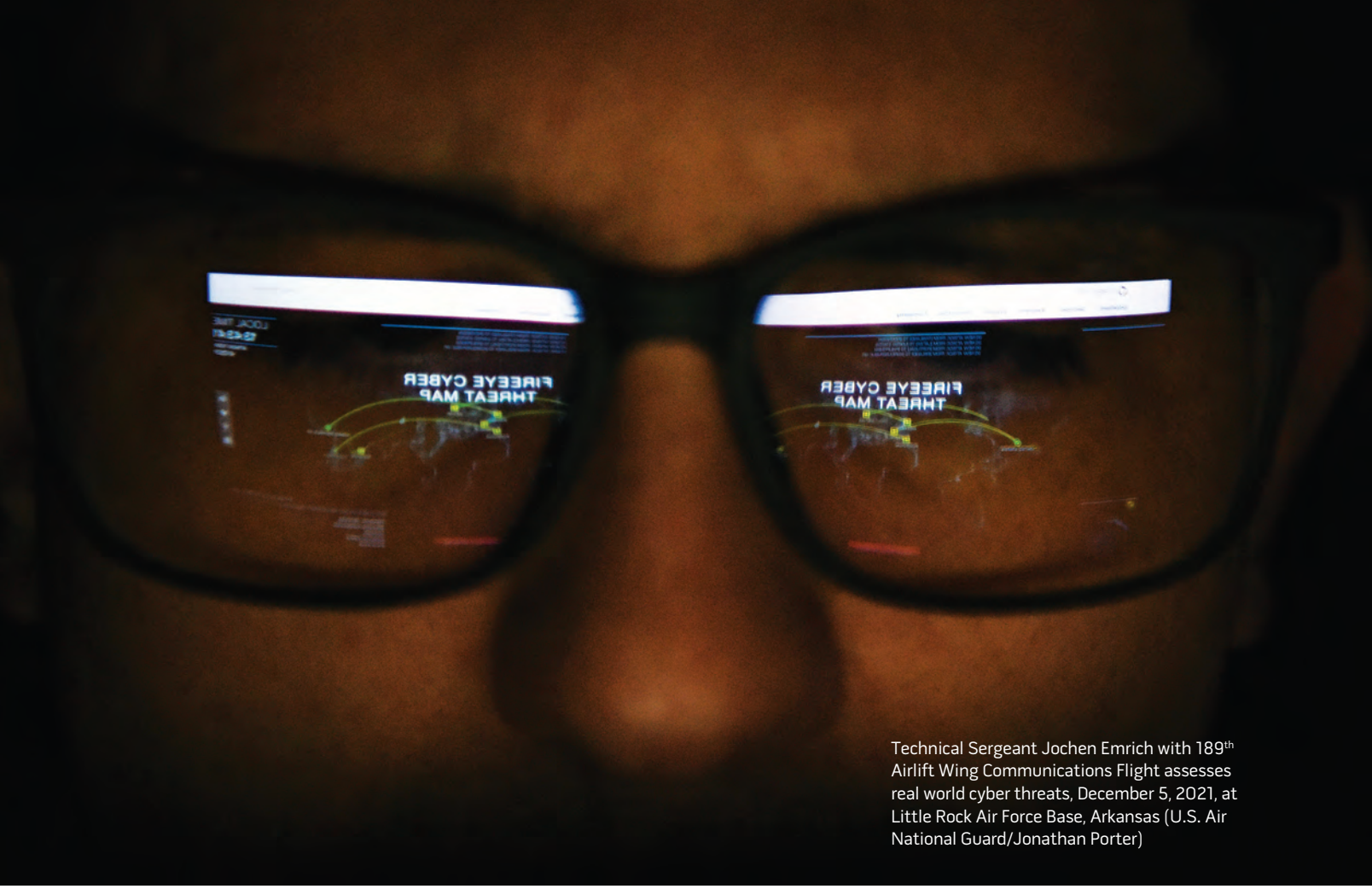


Technical Sergeant Jochen Emrich with 189th Airlift Wing Communications Flight assesses real world cyber threats, December 5, 2021, at Little Rock Air Force Base, Arkansas (U.S. Air National Guard/Jonathan Porter)

Cyber in the Shadows

Why the Future of Cyber Operations Will Be Covert

By Richard L. Manley

Current cyber conflict looks very similar to traditional conflict models. The difference from traditional power dynamics offered by the cyber domain, however, is the asymmetrical advantage of technology for would-be actors. This new element of national power allows weaker actors to "punch above their weight" in competition or conflict with Great Powers in a unipolar or multipolar world. John Arquilla describes this new environment as an "information revolution" that "implies the rise of cyber war, in which neither mass nor mobility will decide outcomes."[1] Continuing in the spirit of Ivan Arreguín-Toft's strategic interaction theory, cyber operations allow significant latitude for strong actors to compete indirectly, short of physical conflict in the traditional sense.[2] Cyber also allows weak actors to impose costs against strong actors without incurring significant risk. Strong actors continue to integrate the effects achieved in the cyber domain into their doctrinal foreign policy, whether militarily or otherwise, to maximize layered effects. The outcomes of the new competitive space of cyber have been theorized for decades now, but what makes prediction difficult is the pace of innovation and the change in available technology.

Special Forces Chief Warrant Officer 3 Richard L. Manley, USA, is a Candidate for a Master of Science in Defense Analysis at the Naval Postgraduate School.

This article discusses the effects of cyber operations on the strategic interaction of actors in the cyber domain, gives examples of the use of cyber in Great Power competition, and explains how cyber operations offer an asymmetric advantage to weaker actors. It focuses on works by Keir Giles, Austin Carson and Keren Yarhi-Milo, and Ryan Maness and Margarita Jaitner toward the use of cyber operations by revisionist state actors such as the Russian Federation and the People's Republic of China. It demonstrates how cyber allows these actors to "play a weak hand well" in support of their respective theories of hybrid warfare and unrestricted warfare. Moving on from revisionist states, this article gives examples of strategic interaction in the cyber domain by rogue states such as North Korea by describing the asymmetric advantage that nation enjoys as the weaker actor in a struggle with South Korea and the United States. Works from Hyeong-wook Boo, Ellen Nakashima, and Paul Sonne enable explanation of how cyber operations allow rogue states to apply pressure on adversaries without necessarily advancing conventional conflict. Finally, in contrast to Arquilla, this article takes the position that, despite the asymmetrical advantages offered by cyber operations, their future use will necessarily be clandestine or covert to avoid crossing the threshold of armed conflict.

Revisionist State Operations

As the Russian Federation continues expansionist aims to its west to thwart North Atlantic Treaty Organization (NATO) expansion in Eastern Europe, the Kremlin understands that the Alliance can mass more combat power and enjoys a spending advantage, should it unite with Eastern European nations. To combat this outcome, Russia has incorporated technology into its traditional form of "active measures" to ensure that psychological operations provide it a deceptive advantage. This ability to use political and psychological warfare allows Russia to create doubt in the minds of both Allies and aspirants. For example, during the incursion into Ukraine in 2014, "Russians cleverly used SMS messages to text Ukrainian frontline troops to demoralize their frontline forces—which even include[d] references to their wives and children back in Kyiv."[3] Adaptation of cyber tactics creates a definite psychological advantage for Russian forces against a distracted and potentially demoralized combatant on the battlefield. By shaping the battlefield through cyber-enabled information operations, Russia can prevent consolidation of an opposing ally's military power and create doubt within alliances.

These strong-arm tactics are not limited only to military capability but are also on full display in the political warfare arena. Russia's efforts to deploy active measures during the 2016 U.S. elections are well reported, and the latent effect is a lasting doubt in the minds of many Americans regarding the validity of the U.S. system. Maness and Jaitner explain that "Russian political interference is about keeping an adversary nation domestically divided for a long period of time. Russia looks to spread division, exacerbate any conflict possible, and ultimately destabilize the political system and erode trust in the government and institutions."[4] Moscow has used this strategy of sowing distrust for decades, but the advantages afforded by the cyber environment will ensure these efforts continue aggressively unless checked.

Along with Russia, China seeks to upset global norms through incorporation of cyber operations. China's concept of unrestricted warfare allows it to combine all elements of national power to pressure opponents, and incorporation of cyber operations certainly allows China to dictate the pace of that competition. After an internal recognition that it was falling behind technologically, the Chinese Communist Party began a worldwide campaign of intellectual property theft to artificially advance its technological horizons. Today, China aggressively targets U.S. military contractors and infrastructure, seeking to improve its capabilities. In his nomination hearing to lead U.S. Indo-Pacific Command, Admiral Philip S. Davidson explained, the "Chinese are investing in a range of platforms, including quieter submarines armed with increasingly sophisticated weapons and new sensors. . . . What they cannot develop on their own, they steal—often through cyberspace."[5] These comments came on the heels of a Chinese hack of a "trove of highly sensitive data on submarine warfare," highlighting the seriousness of Chinese hacking.[6] Despite U.S. pressure and diplomatic interactions, China seems poised to continue its online espionage practices while relying on the entanglement of competitors' economies with its own as security against decisive action to counter it. China's willingness to aggressively use technology to monitor and control its citizens internally while exporting similar technologies to would-be authoritarian states should make these efforts particularly concerning to free nations.

Rogue Actors and Asymmetrical Advantage

Rogue states, such as North Korea and Iran as well as violent extremist organizations, count on the asymmetric advantage offered by operations in cyber space, though with differing levels of success. North Korea's coercive efforts to strong-arm Sony in 2014 led to international recognition that a weak actor can find avenues of coercion in cyber, even if the stated goal of limiting release of the movie *The Interview* failed. But this widely reported attack is a small piece of what Hyeong-wook Boo describes as "very sophisticated cyber attacks against South Korea and the United States. Starting from simple DDoS [distributed denial-of-service] attacks on popular websites and e-mail hacking, their cyber offensive operations adopted advanced technologies called . . . Advanced Persistent Threat."[7] These aggressive attacks are part of North Korea's strategic interaction with a stronger actor. Such risky operations by rogue states are allowed to continue because the stronger actor wishes to keep conflict low. The risk taken by rogue states in the cyber realm is that these operations hinge on the stronger actor's desire to maintain a low-conflict state. Should the strong actor determine

that it is no longer in its interest to allow such activities, and that direct conflict would provide a better alternative to absorbing attacks, the weaker actor cannot hope to prevail. The consequence is that cyber operations must necessarily exist under a threshold of acceptable violence, which limits the decisiveness of a cyber campaign.

Future of Cyber Operations: Movement Toward "Covertness"

The ability to use cyber operations as a shaping mechanism toward a desired policy will require the ability to plausibly deny the actor's involvement. This interaction has been described as the "frontstage and backstage" of international relations where an "action [that] may be unseen or misunderstood by people only viewing the *frontstage* carries amplifying messaging and signaling to those with *backstage* access."[8] The full implication of an action or event is better understood by those with understanding of the backstage who can receive the full message. In this way, a form of communication can take place between a target and a sponsor who remains nonattributed to the activity.

This explains how a stronger actor can incorporate cyber operations into an overall deterrence strategy, but how can a weaker actor hope to accomplish decisive actions in the cyber realm? Because the weak actor is, by definition, less powerful across the spectrum of diplomatic, informational, military, and economic capacity than a stronger competitor, its operations can only exist under an acceptable threshold of violence or pressure. When a strong actor determines that it is no longer in its best interest to allow a weak actor to compete in the cyber realm, what is the weak actor's response? John Gartzke explains the relative risk factor of cyber attacks is "low mainly because those who have the power to intervene to stop or punish irritant behavior often do not have the motivation to do so."[9] This article's position on the growing need to hide cyber activities draws heavily from Gartzke's works revisiting the stability-instability paradox. The distinction lies in the credibility of the weaker actor's capacity to address the response of the stronger. Carson and Yarhi-Milo explain that "covert action is intelligible because it contains a range of salient, qualitative thresholds that are mutually meaningful as symbols of a sponsor's resolve," but they stress that these signals must be "believable."[10] The degree to which a weak actor can credibly signal resolve to a strong actor plays a significant role in defining the stability (or instability) of their interaction.

Stability-Instability Paradox in Cyber

Much of Cold War deterrence theory was built on the concept of mutually assured destruction. Because the consequences of full-scale conflict between nuclear powers were so great, nuclear actors understood that their nuclear might was essentially not a viable strategy except for its deterrent effect. From that deterrent effect was born the stability-instability paradox, which posited that "scaling up nuclear deterrence might actually increase freedom of action at lower levels of violence."[11] From this paradox, Professor Glenn Snyder considered the strategic interaction between the United States and the Soviet Union by hypothesizing that the "Soviets probably feel, considering the massive retaliation threat alone, that there is a range of minor ventures which they can undertake with impunity, despite the objective existence of some probability of retaliation."[12] Because the consequences of action taken to prevent these low-intensity conflicts were so great, the strategic actors naturally settled into a competitive environment where offensive actions were allowed provided that an acceptable threshold was not crossed. The question of the time was: What exactly is the acceptable threshold and how far could an adversary be pushed?

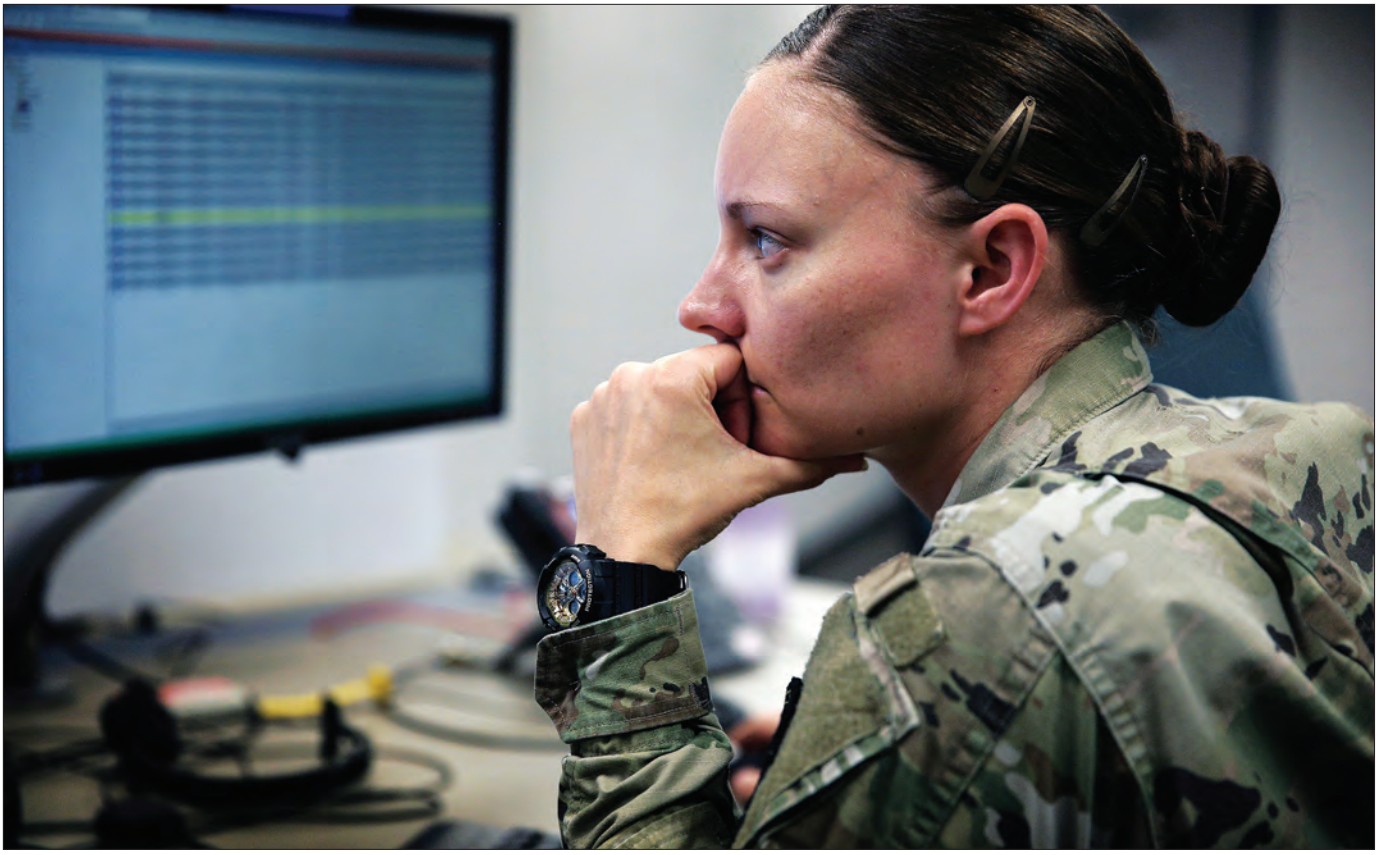
Recently, Gartzke revisited the stability-instability paradox by applying it to the cyber environment. Table 1 interprets that application as it relates to the "covertness" of cyber operations. Assuming the model is true, the following logic unfolds related to the future of cyber operations:

- The United States, as the unipolar actor, can continue to set the terms of cyber operations. When seeking to influence revisionists who are relatively strong and can retaliate, the United States can find an advantage in covertness, provided the backstage message is received. When dealing with rogues, the United States can conduct operations overtly, if desired, to send a clear message for deterrence or covertly if targeting a specific objective or individual. The United States will also dictate the acceptable threshold of activities by determining which cyber attacks it is willing to absorb, and where its cyber "red lines" for retaliation (physical attack) exist.
- Revisionist actors seeking to influence the United States should develop appropriate covert solutions through use of proxies and surrogates to allow for plausible deniability and should ensure their

Table 1. Strategic Interaction Model in Cyber

	Strong Actor	**Weak Actor**
Strong Actor	Covert interaction in cyber	Overt interaction in cyber
Weak Actor	Covert interaction in cyber	Either covert or overt interaction in cyber

Source: Adapted from Michael Krepon, "The Stability-Instability Paradox," *Arms Control Wonk*, November 2, 2010, available at <https://www.armscontrolwonk.com/archive/402911/the-stability-instability-paradox/>.



U.S. Cyber Command Cyber National Mission Force member participates in training and readiness exercise at Fort George G. Meade, Maryland, May 24, 2021 (U.S. Army/Josef Cole)

cyber operations remain under the U.S. thresholds for overt retaliation. In competition with one another or with rogue actors, revisionists can operate either covertly or overtly, depending on the relative conventional strength of their opponent.

- Rogue actors should seek to remain as covert as possible, except in those instances where they determine that public support may limit conventional retaliation from a stronger actor. An example of this is the Sony hack perpetrated by North Korea. While it did not achieve its fully intended aims, North Korea did send a deterrent message to its adversaries and messaged its capabilities effectively.

Cyber Brinkmanship

In October 1962, the two global multipolar superpowers came to the absolute brink of nuclear war over missiles in Cuba. Each world leader faced a seemingly unwavering adversary, and neither John F. Kennedy nor Nikita Khrushchev appeared to have any incentive to compromise first, short of preventing the end of modern civilization. Each nuclear superpower needed to demonstrate to the other and its populace that the terms of competition were being redefined. This redefinition nearly ended the world. What followed after this crisis was a recognition that conflict in the nuclear world was to be different—that superpowers seeking to damage one another had new consequences, and new rules to the game were necessary. The result was an era of covert activities that would allow for indirect pressure while avoiding direct pain. Neither side wanted to repeat the flare-up of the Cuban Missile Crisis, and so both settled into a covert status quo.

Considering the lessons of the beginning of the nuclear age, it seems appropriate to consider similar conditions most likely to exist in the digital age. A period of "feeling out" each other's capabilities seems natural as new norms and standards are defined. It is also natural to assume that some level of brinkmanship will take place in relation to cyber capability. In a piece for *Wired* magazine in August 2019, Andy Greenberg asserted that this brinkmanship is already taking place:

Over the past weekend, the New York Times *reported that U.S. Cyber Command has penetrated more deeply than ever before into Russian electric utilities, planting malware potentially capable of disrupting the grid, perhaps as a retaliatory measure meant to deter further cyberattacks by the country's hackers. But judging by Russia's response, news of the grid-hacking campaign may have already had the immediate opposite effect: The Kremlin warned that the intrusions could escalate into a cyberwar between the two countries, even as it claimed that Russia's grid was immune from such threats.*[13]

The implications of cyber attacks against civilian utility grids are especially concerning based on the risk of widespread loss of innocent lives; while not as outright deadly as a nuclear attack, the level of damage and the follow-on effects are incalculable if conducted in an escalatory fashion. While Russia has folded cyber attacks on a limited to moderate scale into its hybrid warfare strategy, as demonstrated in the Crimea annexation of 2014, neither side fully understands the implications of these types of infrastructure attacks against a peer competitor.

Greenberg goes on to explain that the risk of this cyber brinkmanship may have been brought on by an effort from the Trump administration to signal a deterrent capability to the Russians. Former Homeland Security Advisor Tom Bossert explains that the potential for escalation is particularly important given our own vulnerabilities to attacks on the grid: "If you're doused in gasoline, don't start a match-throwing contest."[14] Herein lies another paradox: How does one signal covert capability? What is the appropriate method to demonstrate a secret?

Covertness Limits Brinkmanship

Since the dawn of the nuclear age, covert action has been the "third option" for policymakers requiring a response to an adversary with whom war is impossible or too costly. According to Carson and Yarhi-Milo, "Using covert action to signal resolve can also appear credible because of its impact on the risk of crisis escalation."[15] This principle has allowed nuclear superpowers to compete with deniability, thus limiting the escalatory impacts of conflict and allowing one another a way out. Examples of this behavior in cyber space are beginning to emerge. The unclaimed Stuxnet attack on an Iranian nuclear subterfuge facility and Russian interference in the 2016 U.S. Presidential election are both examples of nation-state competition in the covert cyber realm. These examples demonstrate the potential of direct covert cyber operations to allow flexibility in policy while affecting an adversary's behavior. But is this the limit of cyber's potential? Are there indirect attack vectors that can set the new tone of conflict in cyber? During the Cold War, a series of proxy conflicts emerged as the battleground for nation-states. Insurgencies and guerrilla war in Iran, Vietnam, Afghanistan, Tibet, and other places were conflict areas where nation-states could impose cost on an adversary and dictate terms of policy. Can the cyber realm provide the next covert battlespace?

The Arab Spring

A case study for the power of online connectivity and the influence of social

Protesters in Tunis, Tunisia, on January 23, 2011, during Jasmine Revolution that toppled former ruler Ben Ali (Idealink Photography)

media exists in the case of the Arab Spring. Erin Blakemore writes:

Beginning in December 2010, anti-government protests rocked Tunisia. By early 2011 they had spread into what became known as the Arab Spring—a wave of protests, uprisings, and unrest that spread across Arabic-speaking countries in North Africa and the Middle East. Pro-democratic protests, which spread rapidly due to social media, ended up toppling the governments of Tunisia, Egypt, Libya, and Yemen.[16]

The pro-democratic protests were fueled through propagation of online messaging. Platforms such as Twitter, Facebook, and YouTube fed a populace eager for change, even after governments attempted to shut down the communications networks. Philip Howard describes the power of social media and online connectivity related to the revolutions: "People who shared interest in democracy built extensive social networks and organized political action. Social media became a critical part of the toolkit for greater freedom."[17]

As of this writing, no nation or entity has claimed responsibility for control of this social media toolkit. The online activist group Anonymous does claim to have provided technical support and expertise, but the messaging and content are assessed to have been spontaneous and homegrown. But what if, in the future, themes and content could be guided? Insurgencies and political actions that formerly required agent interaction may now be propagated through social media, their grievances engineered by the aggressor. Russia's attempts at political manipulation in the 2016 U.S. Presidential election came close to this type of social engineering, but the effects remained mostly in the cyber realm except for a few protests and fights. The social engineering aspects potentially available to a covert cyber operation are significant, especially when considered alongside already established research regarding social movement theory.

In his pioneering works on social movements, anthropologist David Aberle posits that there are four types of social movements. Table 2 illustrates his description of the four types, with an added consideration of a category for vulnerability to cyber influence.

As the Internet took shape as a component of everyday modern life, researchers began to look at the effects of a networked populace and its ability to share grievances. In the late 1990s, as social media was a ground-floor enterprise, Donatella della Porta and Mario Diani defined *social movement* in their foundational work on the subject as "informal networks formed through the shared beliefs and solidarity of members, which mobilize to support specific positions on social issues through various forms of protest."[18] In 2003, Diani further emphasized the effect of social media on movements: "The new social movements that inspired the network model did not require membership, were decentralized, dynamic, and without formal hierarchy, and depended on participants identifying with the perspectives and positions of the movement and its objectives."[19] It is in this description where the opportunities for covert action emerge. A decentralized, leaderless network that ascribes truth to its own interpretations, is motivated through shared belief in those principles, and lacks a clear hierarchy presents an interesting opportunity to either witting or unwitting manipulation.

A motivated state actor, desiring to indirectly affect the actions of a competitor, could capitalize on this type of informal network structure to seed disinformation and deception to build toward social movement. This could be manifested in the social populace of a competitor's ally, key trading partner, commodity supplier, or directly into the populace itself. Propagation of misinformation or amplification of counter-state narratives can allow for frontstage condemnation and pressure, all while

Table 2. Four Types of Social Movements

Movement Type	Focus of movement	Examples	Vulnerability to cyberinfluence	Examples of cybervulnerability
Alterative	Partial individual change	Mothers Against Drunk Driving	High—individuals are easily manipulated by social media	Anti-vaxxers, Tide POD eaters, birther movement
Redemptive	Total individual change	Religious movement	Medium—group change is difficult without a counterstate narrative	White nationalists, lone-wolf terrorists, Antifa members
Reformative	Partial social change	Women's suffrage movement	Medium—affecting existing groups with common grievances is easier than convincing people to change groups	U.S. political parties, sports fans
Transformative	Total social change	Revolutions	Low—total social change requires actions outside of the cyber realm. Cyber is an enabling function and can engineer the environment for grievances to manifest	2016 U.S. elections, Arab Spring, Russian cyber-efforts in Crimea

Source: Nick Lee, "The Four Types of Social Movements," *Medium,* August 2, 2019, available at <https://medium.com/@nicklee3/the-four-types-of-social-movements-8db910192573>.

controlling the narrative through covert action in the backstage. While this is not new to the concept of covert action, it is a new method of distribution and a new opportunity to act covertly using unwitting proxies. In the Arab Spring example, it is not impossible to imagine a state or group of states motivated by promulgation of democracy controlling the messaging to Tunisia, Egypt, and Syria covertly, manipulating the tone, tempo, and spread of counter-state narratives the same way a military general coordinates a campaign. In this manner, a covert actor can adjust the tenor and content of messaging in the backstage to either ratchet up pressure when hard negotiations are happening or dial it back when concessions are made—all while maintaining plausible deniability about involvement and managing escalatory risk.

Conclusion

As society comes to terms with the realities of a cyber-enabled world, the consequences of cyber attacks will most likely increase as strong actors seek to deter their weaker adversaries. The advantage that cyber attacks afford weaker actors can be mitigated through consequences in the physical space. These consequences will most likely drive cyber competition toward covert activities conducted through proxies and surrogates. The effects of cyber operations will seek to shape the environment for a competitive advantage in conflict, but the results of cyber operations will most likely not be decisive outcomes. Instead, cyber operations will be incorporated into other forms of strategic interaction, including wartime functions, as a supporting effort, much the same way current covert action is incorporated as a policy-shaping mechanism. The potential of covert social movement and manipulation outweighs the risk of overt actions, either cyber or war. The risk calculus weighs heavily into the covert realm, even if only as a shaping action with potential for full-scale success.

The net benefits of indirect cyber operations are a potential outlet for actors to compete in a nonlethal way, continuing the trend of making warfare more precise and leading away from large-scale loss of life. The threat is the limiting effect that security requirements have on the technology surrounding a modern world and the vulnerabilities that exposure to cyber operations creates in a hyper-connected planet. The opportunities to engineer an environment to promote social change from within an adversary's borders, while managing escalation potential, demonstrate that covert cyber operations are a growth industry for both strong and weak actors. **JFQ**

Notes

[1] John Arquilla, "Cyberwar Is Already Upon Us," *Foreign Policy*, February 27, 2012, available at <https://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/>.

[2] Ivan Arreguín-Toft, "How the Weak Win Wars: a Theory of Assymetric Conflict," *International Security* 26, no. 1 (Summer 2001), available at <https://web.stanford.edu/class/polisci211z/2.2/Arreguin-Toft%20IS%202001.pdf>.

[3] Keir Giles, "Assessing Russia's Reorganized and Rearmed Military," Carnegie Endowment for International Peace and the Chicago Council of Global Affairs, Task Force on U.S. Policy Toward Russia, Ukraine, and Eurasia, May 4, 2017, available at <https://carnegieendowment.org/files/5.4.2017_Keir_Giles_RussiaMilitary.pdf>.

[4] Ryan C. Maness and Margarita Jaitner, "There's More to Russia's Cyber Interference than the Mueller Probe Suggests," *Washington Post*, March 12, 2018, available at <https://www.washingtonpost.com/news/monkey-cage/wp/2018/03/12/theres-more-to-russias-cyber-meddling-than-the-mueller-probe-suggests/>.

[5] Ellen Nakashima and Paul Sonne, "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare," *Washington Post*, June 8, 2018, 5.

[6] Ibid.

[7] Hyeong-wook Boo, "An Assessment of North Korean Cyber Threats," in *The Kim Jong Un Regime and the Future Security Environment Surrounding the Korean Peninsula* (Tokyo: National Institute for Defense Studies, 2017), available at <http://www.nids.mod.go.jp/english/event/symposium/pdf/2016/E-02.pdf>.

[8] Austin Carson and Keren Yarhi-Milo, "Covert Communication: The Intelligibility and Credibility of Signaling in Secret," *Security Studies* 26, no. 1 (January 2, 2017), 124–156, available at <https://doi.org/10.1080/09636412.2017.1243921>.

[9] Jon R. Lindsay and Erik Gartzke, "Coercion Through Cyberspace: The Stability-Instability Paradox Revisited," in *The Power to Hurt: Coercion in Theory and in Practice*, ed. Kelly M. Greenhill and Peter J.P. Krause (Oxford: Oxford University Press, 2018), 40.

[10] Carson and Yarhi-Milo, "Covert Communication."

[11] Michael Krepon, "The Stability-Instability Paradox," *Arms Control Wonk*, November 2, 2010, available at <https://www.armscontrolwonk.com/archive/402911/the-stability-instability-paradox/>.

[12] Glenn Herald Snyder, *Deterrence and Defense* (Princeton: Princeton University Press, 2016).

[13] Andy Greenberg, "How Not to Prevent a Cyberwar with Russia," *Wired*, June 18, 2019, available at <https://www.wired.com/story/russia-cyberwar-escalation-power-grid/>.

[14] Ibid.

[15] Carson and Yarhi-Milo, "Covert Communication."

[16] Erin Blakemore, "What Was the Arab Spring and How Did It Spread?" *National Geographic*, March 29, 2019, available at <https://www.nationalgeographic.com/culture/topics/reference/arab-spring-cause/>.

[17] Catherine O'Donnell, "New Study Quantifies Use of Social Media in Arab Spring," *UW News*, September 12, 2011, available at <https://www.washington.edu/news/2011/09/12/new-study-quantifies-use-of-social-media-in-arab-spring/>.

[18] David Zimbra, Ahmed Abbasi, and Hsinchun Chen, "A Cyber-Archaeology Approach to Social Movement Research: Framework and Case Study," *Journal of Computer-Mediated Communication* 16, no. 1 (October 1, 2010), 48–70, available at <https://academic.oup.com/jcmc/article/16/1/48/4067637>.

[19] Ibid.