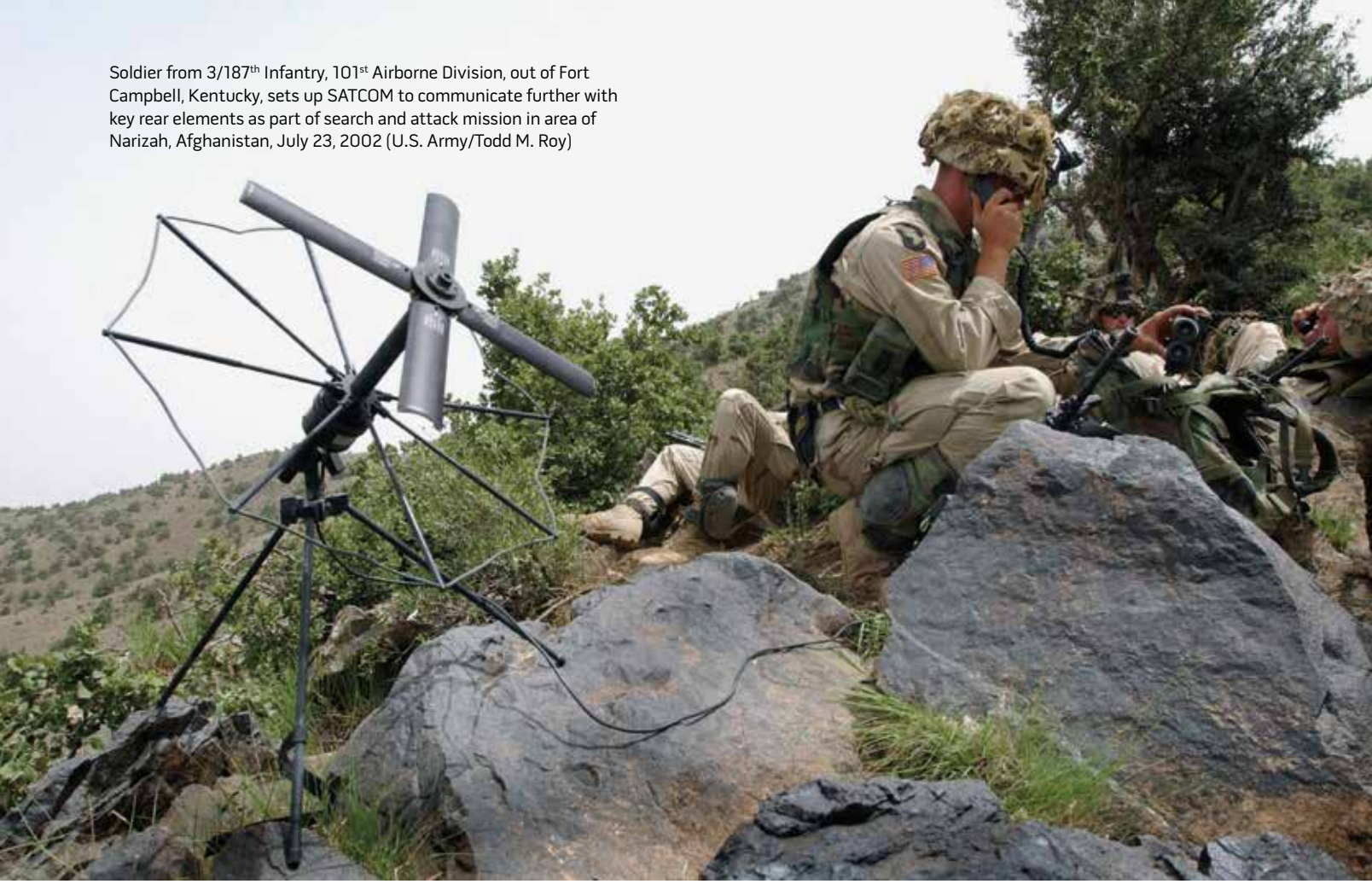


Soldier from 3/187th Infantry, 101st Airborne Division, out of Fort Campbell, Kentucky, sets up SATCOM to communicate further with key rear elements as part of search and attack mission in area of Narizah, Afghanistan, July 23, 2002 (U.S. Army/Todd M. Roy)

Applying Irregular Warfare Principles to Cyber Warfare

By Frank C. Sanchez, Weilun Lin, and Kent Korunka

The cyberspace threat exists in a realm that does not conform to the physical limits of land, sea, air, and space. Unlike these traditional domains, cyberspace fosters an unpredictable threat that can adjust, morph, and reproduce without a national identity or face.[1] The challenge of the military is to posture its approach to cyberspace and cyberspace threats that are initiated by faceless, borderless, and sometimes nationless enemies. These enemies manifest in a domain neither confined nor governed by the traditional norms and rules of war, which the broader military has no experience undertaking. To ensure the United States maintains cyberspace dominance and can foresee, rapidly respond to, and counter cyberspace threats, the U.S. military's strategy and approach to cyberspace must adapt and incorporate unconventional approaches and hybrid warfare into its operational capability.

Despite its importance, the Nation's leaders, strategists, and military planners struggle to understand how cyberspace operations (CO) fit into national security as an instrument of national policy. A significant shortcoming is due to the leaders' lack of experience and basic understanding of what cyberspace is and what effects can be achieved in the cyber

Commander Frank C. Sanchez, USN, is an Action Officer on the Joint Staff J32, Intelligence, Surveillance, and Reconnaissance Operations. Major Weilun Lin, USAF, is Chief of the Central and South Asia Branch, Joint Cyberspace Center, U.S. Central Command. Lieutenant Colonel Kent Korunka, USA, is a Joint Intelligence Planner, Joint Planning Support Element, Joint Enabling Capabilities Command, U.S. Transportation Command.

Table. Conventional, Cyber, and Irregular Warfare

	Conventional	Cyber	Irregular
Purpose (why)	Gaining political, economic, ideological, social, and religious dominance via geolocation dominance for a period of time	Assisting in gaining political, economic, ideological, social, and religious dominance; gaining information for competitive advantage	Assisting in gaining political, economic, ideological, social, and religious dominance; gaining information for competitive advantage
Strategy (how)	Using overt operations and/or covert operations; showing might; little attribution issue	Using overt operations and/or covert operations; attribution issue	Using covert operations; attribution through intelligence
Involvement (who)	Some people such as military or paramilitary personnel	Everyone who has a device connected to affected networks	State and nonstate actors, adaptive adversaries such as terrorists, insurgents, and criminal networks
Targets (what)	Humans; mainly tangible objects; directly affecting human life	Mainly intangible items such as information or tangible items such as information systems; may indirectly affect human life in cyber physical cases	Humans; mainly tangible objects; directly affecting human life
Space (where)	Limited geolocaion	Anywhere with respect to geolocation if connected	Global
Duration (when)	A limited period of time	Ongoing, but one attack is usually within a short period of time	Very limited period of time
Preparation time (when)	Relatively long period of time	Relatively short period of time	Relatively short period of time
Cost (what)	Expensive	Relatively less expensive	Relatively less expensive
Characteristics (what)	Relatively more transparent	Relatively opaque and in stealth mode	Relatively opaque and in stealth mode
Attribution (what)	Relatively easy to find out	May be hard to find out	Relatively difficult to find out
Rules of engagement (what)	Relatively clear	Not clear	Not clear
Impression (what)	Always severe or brutal; obvious	Less severe if not life or death situation; sometimes not felt	Less severe if not life or death situation; sometimes not felt
Damage (what)	Severe with physical casualty	Severe with information loss	Sometimes severe
Direct impact upon (who)	Someone/some businesses	Everyone/every business connected to affected networks	Someone/some businesses
Impact based on (where)	Geolocation	Connection	Geolocation
Deterrence (what)	Obvious and forceful	Limited currently	Subtle
Dominance (what)	Could be achieved	Hard to achieve	Hard to achieve
Result/Gain (what)	Obvious	May not be very clear	May not be very clear
Winner (who)	Clear to identify	May be hard to decide	May be hard to decide
Time for recovering (when)	Relatively long	Relatively short	Relatively short

Source: Adapted from Jim Chen and Alan Dinerman, "On Cyber Dominance in Modern Warfare," in *Proceedings of the 15th European Conference on Cyber Warfare and Security*, ed. Robert Koch and Gabi Rodosek (Reading, UK: Academic Conferences and Publishing International Limited, 2016), 54.

realm. Unlike the younger generation, who are considered digital natives, the majority of national and military leaders and military planners are considered digital immigrants. Popularized by Marc Prensky, the phrase *digital natives* refers to the generation who grew up using digital technology, and *digital immigrants* refer to the generation born before the advent of technology (circa the 1980s) but later adopted its use.[2] While digital immigrants lack cyber knowledge, many of them understand irregular warfare (IW) and the value and importance of special operations. The many similarities shared by IW and cyber warfare (CW) can establish a foundation to guide U.S. leaders in the execution of cyberspace operations to maintain cyber superiority.

Early cyber power theorists generally recognized three key terms: *cyberspace*, *cyber power*, and *cyber strategy*.[3] As the cyberspace domain matures, cyber theorists and thinkers still have not reached the appropriate definitions of these key terms. An understanding of irregular warfare fosters a rudimentary knowledge of cyber warfare. By highlighting how irregular warfare and cyber warfare are similar and providing the critical framework for using IW principles to approach, define, and integrate cyberspace operations across all domains and Services, U.S. leaders can begin to understand how cyber power can increase the effectiveness of the broader U.S. military cyber force.

Irregular Warfare and Cyber Warfare Interlinked

Special operations have a long, storied, and varied history within the U.S. military, including, for example, Roger's

Rangers, the assault of Pont-du-hoc, and Operation *Eagle Claw*. Colonel Joseph Celeski, USA (Ret.), noted that the Joint Special Operations University Special Operations Forces (SOF)-Power Workshop concluded that special operations is "a multi- and cross-domain force, capable of conducting or supporting conventional or unconventional operations on various levels leading to or supporting military and political outcomes."[4] Members of the workshop listed the following characteristics of the SOF operational environment:

- A complex operating environment marked by instability and ambiguity; acts of violence, influence, and leverage are conducted in a nonlinear and often indirect way and include low-level operations of subtlety and guile.[5]
- A high-risk, highly sensitive environment, in which there is high personal and political risk in conducting operations.[6]
- An irregular warfare environment characterized by intra-state and substate acts of political violence, plus insurgency, subversion, violent political action, and terrorism.[7]

Joint Publication 3-05, *Special Operations*, described the special operations environment as "hostile, denied, or politically and/or diplomatically sensitive . . . and . . . characterized by one or more of the following: time-sensitivity, clandestine or covert nature, low visibility, work with or through indigenous forces, greater requirements for regional orientation and cultural expertise, and a higher degree of risk."[8]

Cyberspace shares similarities with special operations due to its complexity and actors. The new global domain of cyberspace relies on the connected information technology infrastructure that includes all the automation and networked system components through which information or content flows or is stored.[9] Cyberspace operations are conducted in the physical network, logical network, and cyber-persona layers of the cyberspace domain.[10] The ease of entry into cyberspace allows individual actors, criminal organizations, and small groups to operate in the cyberspace environment on a similar level as nation-states and transnational organizations. The anonymity and lack of attribution afforded actors in the cyberspace domain resemble the covert or clandestine aspects of SOF.

The cyber domain threatens regional and national security in ways that are uncommon in the other traditional domains of land, sea, air, and space.[11] As a result, bad actors in cyberspace range from individual hackers and criminal enterprises to violent extremist organizations and nation-states. Bad actors steal information for personal or national gain for reasons that include profit, intelligence, denial of services, or to inflict damage on critical infrastructure. Within the traditional domains, these types of actions are relatively recognizable and easier to classify as acts of war, but in cyberspace the underlying intent and attribution of a cyber attack are difficult to discern.

Past thinkers and strategists have identified other similarities between special operations and cyber operations. Eric Trias and Bryan Bell wrote, "The inherently clandestine nature of special operations parallels the ease of conducting stealthy cyber operations."[12] Patrick Duggan proposed that "cyber-warfare is, at its core, human-warfare" and "requires SOF's unique human expertise, unconventional mindsets, and discreet asymmetric options."[13] Most notably, Jim Chen and Alan Dinerman presented a framework to compare and contrast the similarities between conventional warfare and cyber warfare. Using factors borrowed from other authors, Chen and Dinerman created a matrix to facilitate the discussion of the cyber warfare capabilities compared to conventional warfare.[14] An adaptation of their findings is reflected in the table, which includes IW for comparison and contrast, in order to highlight the similarities between CW and IW. While not entirely inclusive of all aspects and characteristics of each warfare, the table illustrates the strong parallels between cyber warfare and irregular warfare.

Despite the many similarities highlighted in the table, it is important to recognize the differences between CW and IW. A key difference, low personal risk, is the greatest strength of cyber warfare. Cyber attacks can be conducted from almost anywhere while still within the confines and relative safety of a nation-state's geographical boundaries. The low personal risk of CW lies in stark contrast to the high personal risk assumed by SOF personnel conducting missions in highly contested environments or deep behind enemy lines. The low personal risk of CW is further supported by the ease of entry into cyberspace and the lack of attribution so long as appropriate steps are taken to conceal identities.

Many core activities of special operations seamlessly fold into the context of cyberspace missions. Offensive cyberspace operations are similar to the intent of special operation's direct action, countering weapons of mass destruction, military information support operations, and special reconnaissance missions. Likewise, the intent of special operation's foreign internal defense and security force assistance missions compare to defensive cyberspace operations.[15] While the cumbersome process to identify and attribute the actor, target, and effect of cyber attacks and information to a nation or group is significant, the necessity for overt nation-state versus nation-state engagement is not as profound. Operations in cyberspace should espouse undetected intrusion where the potential for monitoring, destabilizing, and manipulating provides greater long-term gain than immediate destruction or devastation.

The U.S. approach to CW would likely best benefit from mirroring special operations, IW, and the SOF community, which rely on highly specialized and unique tactics, techniques, procedures, and equipment. At its core, irregular warfare is about the "highly adaptive actors." Rain Ottis and Peeter Lorents wrote, "Cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems."[16] They stress the fact that "cyberspace is an artificial space, created by humans for human purposes," which requires the need to understand and influence peoples' thoughts and actions.[17]

Soldier assigned to 2nd Armored Brigade Combat Team, 1st Cavalry Division, conducts dismounted electronic warfare training at Fort Hood, Texas, August 29, 2018 (U.S. Army/Carson Petry)

Applying Other IW Principles to Cyber

Because of the similarities, the next logical step is to cross over special operations and IW terminologies to build on the foundation of thought and theory regarding cyber warfare. In the paper "Adapt Special Operations Principles to Cyber," Nicholas Co recommended the application of SOF Truths, created by Colonel Sid Shachnow, USA, in the mid-1980s, as guiding principles that will support success in future cyberspace operations.[18] The special operations construct is built on individuals, small units, and advanced technology. The first SOF Truth recognizes that its personnel rather than the equipment are what gives special operations its decisive edge. It is highly trained people applying highly specialized skills with flexibility, creativity, and innovation along with unique capabilities that achieve national objectives across a wide array of military options.[19] Along those lines, the article introduces several other concepts and terminologies adapted from the SOF community.

First, the concept of relative superiority used in irregular warfare should be applied to cyberspace operations. In his book *Spec Ops*, Admiral William McRaven defined the term *relative superiority* as "a condition that exists when an attacking force, generally smaller, gains a decisive advantage over a larger or well-defended enemy."[20] As noted earlier, ease of entry into the cyberspace domain requires low personal risk as it enables a force as small as an individual hacker to overwhelm or operate against a well-defended adversary at a potential point in time. A common misconception exists that global cyber dominance or supremacy is possible and easily maintained. William Bryant quoted the argument from noted cyber expert Martin Libicki that "cyber supremacy is meaningless and, as such, is not a proper goal for operational cyber warriors."[21] The Joint Operating Environment 2035 envisions a future security environment full of vulnerable points through which weapons systems can be directly engaged and military operations have global reach to individual work stations, servers, routers, or controller chipsets.[22] The broad and dynamic nature of cyberspace, consisting of countless devices, makes it impossible to maintain total cyber superiority. This is a persistent risk where at any point in time, one may lose relative superiority. The recent release of U.S. Cyber Command's "Command Vision" highlighted this by stating, "New vulnerabilities and opportunities continually arise as new terrain emerges. No target remains static; no offensive or defensive capability remains indefinitely effective; and no advantage is permanent. The well-defended cyber terrain is attainable but continually at risk."[23] In Air Force Doctrine Document 3-12, *Cyber Operations*, the Air Force defines *cyberspace superiority* as "the operational advantage in, through, and

from cyberspace to conduct operations at a given time and in a given domain without prohibitive interference."[24] This definition closely aligns with Admiral McRaven's comment that relative superiority is achieved at the *pivotal moment in an engagement*.[25]

Second, the term *superiority* alludes to the ability to project a type of power on an adversary—*cyber power*. But the Department of Defense (DOD) does not have a definition of cyber power. The closest DOD definition is the Air Force's definition of *cyberspace force application* as "combat operations in, through, and from cyberspace to achieve military objectives and influence the course and outcome of conflict by taking decisive actions against approved targets."[26] To define *cyber power*, John Sheldon uses the following: "the ability in peace and war to manipulate perceptions of the strategic environment to one's advantage while at the same time degrading the ability of an adversary to comprehend that same environment."[27] By adapting SOF concepts and terminology to these previous definitions, this article proposes the following definition as a springboard for additional thought and discussion on cyber power. At the strategic level, cyber power is the combined strength of a nation's cyberspace capabilities to conduct and influence activities in, through, and from cyberspace to achieve national security objectives in peacetime and across the full spectrum of conflict. At the operational and tactical level, it is also the control and relative superiority gained by application of cyberspace operations over an adversary that uses technology as a means to contest integrity, confidentiality, security, and accessibility of information.

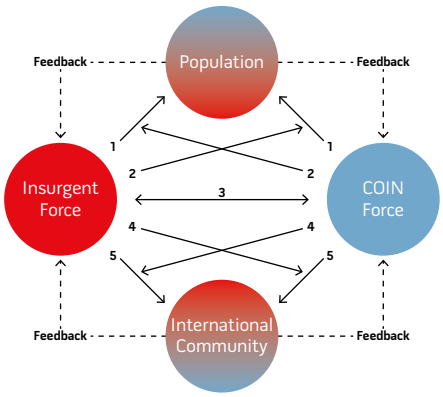
Irregular Framework for Cyberspace Strategy

Today there is a multitude of perspectives and frameworks for cyber strategy. The operational environment influences strategy because strategy must anticipate the changes in the operational environment.[28] DOD utilizes central aspects of the cyber threat such as threat actors, insider threats, supply chain vulnerabilities, and threats to DOD operational ability for developing its strategy for cyberspace operations.[29] Some strategies are only oriented toward cyber defense or cyber security while other strategies are offensive in nature. Principles and theories from Gordon McCormick's "Counterinsurgency Diamond Model" can be applied as a framework for developing a holistic approach or strategy for cyberspace operations. For this article, a brief explanation of McCormick's model in its context and framework would allow application of its overall premise to cyberspace. As shown in figure 1, Greg Wilson briefly describes the model's utilization and interactions:

The Diamond Model establishes a comprehensive framework that considers the interactions between the state or host-nation government, the insurgents or terrorists, the local populace, and international actors or sponsors. The state or the "host nation" government's goal is to destroy the insurgents or limit their growth and influence to a manageable level. The insurgent or terrorist goal is to grow large enough to destroy the state's control mechanisms and replace the existing government or force some form of political concession from the government that achieves their desired goals. To develop an effective strategy, the state must first understand its advantages and disadvantages relative to the insurgents. The state, which normally has an established security apparatus consisting of armed forces and police, has a force advantage over the insurgents but suffers from an information disadvantage. This information disadvantage stems from the fact that the insurgents or terrorists are difficult to detect and target because they are dispersed and embedded in the local populace.[30]

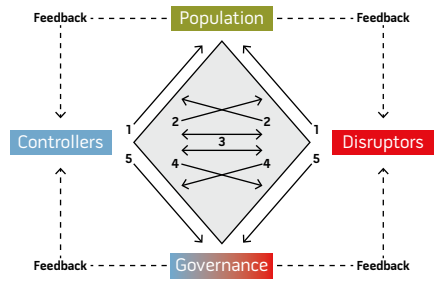
The Cyberspace Diamond Model, shown in figure 2, is based on McCormick's Counterinsurgency Diamond Model and promotes information legitimacy in cyberspace through good governance, improved security, and transparency (as related to attribution). Information legitimacy is at the heart of the cyberspace conflict, as it is received and perceived by all actors within the

Figure 1. McCormick's Counterinsurgency Model



Source: Gordon H. McCormick, "Seminar in Guerrilla Warfare," Naval Postgraduate School, Monterey, CA, 2003.

Figure 2. Cyberspace Diamond Model



Source: Adapted from McCormick's Mystic Diamond Model (McCormick, "Seminar in Guerrilla Warfare," Naval Postgraduate School, Monterey, CA, 2003).

operational environment. National leaders and military professionals should utilize this Cyberspace Diamond Model to frame their strategic approach to cyber warfare. This framework, however, can also be implemented at the operational and tactical levels to aid military leaders and planners in translating strategic direction into operational plans.

The Controllers. Controllers are the current influential or administrative force of a section of cyberspace, or information communication technology (ICT). Examples of controllers can range from network administrators to national governments. Generally, there is a single force that is the lead, but the private sector, organizations, or countries can provide additional capabilities to augment the controllers. The controllers

Air Force Institute of Technology students listen as professor (right) explains hacking technique during class at Wright-Patterson Air Force Base, Ohio, February 20, 2018 (U.S. Air Force/Al Bright)

must integrate all instruments of national power—civil, military, diplomatic, information, economic, technology, and financial. These forces include but are not limited to policymakers, military, law enforcement, intelligence, infrastructure providers, and cyber security personnel. Controllers are defined by the disruptor's perceptions, but external forces can be perceived by the disruptors as influencing the situation, and, consequently, those forces become part of the controllers. The same is true of the controllers defining the disruptors; however, the controllers typically have a greater burden of proof as dictated by global perceptions. Attribution is the greatest hurdle for the controllers to overcome.

The Disruptors. Disruptors are the humans, machines, governments, and criminals conducting or supporting operations to interrupt or disturb the availability, security, confidentiality, or integrity of information in cyberspace. Disruptors are also anyone or anything that is either actively or passively *supporting* disruptors. There is not always a clear distinction between voluntary disruptors and those coerced into supporting disruptors. For example, computers in a botnet that are maliciously controlled without the owners' consent can be considered coerced (involuntary) disruptors. Disruptors conduct exploitation of the population's trust to gain support or control.

The Population. The population consists of the user in cyberspace or the ICT—humans or machines. While support may be coerced out of the population, the population is not considered disruptors until it provides additional support beyond what is required. The population serves as the source of power in both diamond models. However, in cyberspace, the operational environment extends past geographic borders where the population can be global, regional, or an individual system user.

Governance. Although cyberspace lacks the normal rule of law and traditional notion of governance, this article incorporates the term of governance based on the United Nations Educational, Scientific, and Cultural Organization's (UNESCO's) definition. UNESCO defines it as "*structures and processes* that are designed to ensure accountability, transparency, responsiveness, rule of law, stability, equity and *inclusiveness, empowerment, and broad-based participation*."[31] UNESCO also refers to it as "the norms, values and rules of the game" and "about the culture and institutional environment in which citizens and stakeholders interact among themselves and participate in public affairs."[32] As one of the actors in the Cyberspace Diamond Model, governance consists of external nation-states, international organizations, and other groups that do not function in a direct or indirect support role for the controllers and disruptors. Members of the governance, similar to the population, remain neutral until they provide support to a side; once support is provided (or perceived to be provided), they become controllers or disruptors.

The legitimacy of an organization or entity may be placed upon or perceived by the actors within cyberspace. Examples of governance, perceived or placed upon by the population, are the National Institute of Standards and Technology, WikiLeaks, or Hypertext Protocol.

Framing Cyber Strategy and Feedback

Controllers and disruptors must conduct every operation in consideration of how it will affect the perceived legitimacy of the information that is received by the population and governance. As shown and numbered on the Cyberspace Diamond Model, the controllers and disruptors will use all five of the following strategies throughout the cyberspace conflict; however, the source of power, as noted, is primarily the population. Cyberspace enables controllers to focus on direct action against the disruptors by utilizing cyber attacks. It is important to note, however, that controllers must recognize the significance of maintaining the security, accessibility, integrity, and confidentiality of the population's information. As a result, emphasis is placed on strategies 1 and 5 as both forces must execute elements of each strategy.

Strategy 1: Population Support. In figure 2, the intent of strategy 1 is to gain the support of the source of power-—the population—since both controllers and disruptors rely on popular support for success. Although controllers are generally strong in resources, personnel, and cyberspace capabilities, they normally lack specific intelligence on the disruptors. Therefore, controllers need popular support to gain the required intelligence to identify the disruptors. This is similar to the IW interaction between the counterinsurgency or insurgency forces and the population. Controllers promote information legitimacy through good governance, improved security, and socioeconomic conditions in cyberspace. The goal of controllers is to maintain its control of the operational environment, the legitimacy of their information, and the trust of the population. Securing and maintaining the support of the population will cost the controllers a substantial amount of resources, time, capabilities, and manpower.

Building 92 at Microsoft Corporation headquarters in Redmond, Washington, May 30, 2016 (Courtesy Coolcaesar)

Strategy 2: Information Disruption. As depicted in figure 2, the intent of strategy 2 is to prevent or interrupt the opponent's control of the population. The objective of the controllers is to create a divide between the disruptors and population by delegitimizing the disruptors' information and denying them access and freedom of movement to, from, and through the population and other resources in the operational environment. Disruptors must attempt to delegitimize information transmitted through cyberspace and ICTs or break or disrupt the controllers influence over the population and resources that disruptors depend on. Strategy 2 favors the disruptors due to ease of attack on the information legitimacy of the controllers as compared to the challenging task of the controllers to attack the information legitimacy of the disruptors. Transparency and accountability are key to the success of the controllers. Similar to IW, it is easier for insurgents to attack the legitimacy and control of governments.

Strategy 3: Direct Action. Strategy 3 is directed at striking the opponent to disrupt his operations and deny his will and ability to continue the conflict. The controllers' broad, sweeping, and obvious signature enables the disruptors to identify the activities and locations of controllers, which therefore increases the level of personal risk to the controllers. This knowledge enables disruptors to conduct attacks at the time and location of their choosing, thereby potentially reducing collateral damage or attribution. Because the operational environment can be expansive, controllers must first gain intelligence before it can conduct effective operations against disruptors. Indiscriminate assaults can delegitimize the governance of the ICTs and thereby lose the support of the population. An example of indiscriminate assaults is a government's mass censorship of information in cyberspace.

Strategy 4: Disrupt Interaction. Both forces require perceived legitimacy to obtain support and access to governance in strategy 4. The recent Shadow Brokers (disruptors) leak of National Security Agency secrets and capabilities serves to disrupt information legitimacy between the U.S. Government (controllers) and Microsoft (governance). Microsoft has perceived governance because it is responsible for providing vulnerability and security patching and fixes for its products. Using the Cyberspace Diamond Model, the U.S. Government (controllers) needs to attack

the information legitimacy of the Shadow Brokers (disruptors), while boosting their relationship, interaction, and trust with Microsoft (governance).

Strategy 5: Governance Relationship. Strategy 5 outlines that at the nation-state level, the legitimacy of governance and strong international backing can provide perceived information legitimacy. At that level, this is stressed through the whole-of-nation approach and strong international cooperation. The global interlink of cyberspace and ICTs are only as strong as its weakest and most vulnerable link.

Feedback. Feedback is critical in understanding the effects of controllers' and disruptors' actions on popular and international perceptions. The feedback connections allow both forces to assess the success or failure of their cyberspace operations toward information legitimacy. Both sides must establish and maintain feedback mechanisms to assess their operations.

Recommendations and Conclusion

Despite the establishment of U.S. Cyber Command to engage and operate in the youngest warfighting domain, a precise understanding of cyberspace and operations within still remains elusive. The lack of understanding can lead to a miscalculation in the use of cyber forces and capabilities in execution or support of national objectives. Cyber theorists and national leaders must recognize how IW concepts and theories can be applied to cyberspace operations. The basis of their similarities lies in their complexity, highly adaptive actors, and operational environment, which is not limited by traditional geographic boundaries. By comprehending the similarities between CO and IW characteristics, principles, and theories, leaders at the strategic, operational, and tactical levels can frame their thought process and formulate coherent plans.

Through the IW lens, our leaders begin to understand that cyber warfare can be conducted in combination with or independent of conventional military operations. Cyberspace operations against state and nonstate actors should be conducted in protracted regional and global campaigns, often beneath the threshold of overt war.[33] Furthermore, our cyber strategies require a whole-of-nation and/or a whole-of-international-coalition approach to obtain relative superiority in the dynamic cyberspace operational environment. By utilizing the Cyberspace Diamond Model to frame cyberspace strategy at the strategic, operational, and tactical levels, military leaders and planners can translate strategic direction into operational plans for the cyber domain. **JFQ**

Notes

[1] Patrick Lichty, *Variant Analyses Interrogations of New Media Art and Culture* (Amsterdam: Institute of Network Cultures, 2013), 54.

[2] Marc Prensky, "Digital Natives, Digital Immigrants," *On the Horizon* 9, no. 5 (October 2001).

[3] Sean Charles Gaines Kern, "Expanding Combat Power Through Military Cyber Power Theory," *Joint Force Quarterly* 79 (4th Quarter 2015).

[4] Joseph Celeski, *A Way Forward for Special Operations Theory and Strategic Art*, Joint Special Operations University SOF-Power Workshop, August 2011, MacDill Air Force Base, 15.

[5] Ibid., 15–16.

[6] Ibid.

[7] Ibid., 16.

[8] Joint Publication (JP) 3-05, *Special Operations* (Washington, DC: The Joint Staff Staff, 2014), ix.

[9] JP 3-12 (R), *Cyberspace Operations* (Washington, DC: The Joint Staff Staff, 2013), I-2.

[10] Ibid.

[11] Ibid., I-7.

[12] Eric D. Trias and Bryan M. Bell, "Cyber This, Cyber That . . . So What?" *Air & Space Power Journal* 24, no. 1 (Spring 2010), 95.

[13] Patrick Duggan, "Why Special Operations Forces in U.S. Cyber-Warfare?" *Cyber Defense Review*, January 8, 2016.

[14] Jim Chen and Alan Dinerman, "On Cyber Dominance in Modern Warfare," in *Proceedings of the 15th European Conference on Cyber Warfare and Security*, ed. Robert Koch and Gabi Rodosek (Reading, UK: Academic Conferences and Publishing International Limited, 2016), 54.

[15] JP 3-12 (R), *Cyberspace Operations*, vii.

[16] Rain Ottis and Peeter Lorents, "Cyberspace: Definition and Implications," Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 268.

[17] Ibid.

[18] Nicholas Co, "Adapt Special Operations Principles to Cyber," U.S. Naval Institute *Proceedings* 143, no. 6 (June 2017), 58–59.

[19] JP 3-05, *Special Operations*, I-2.

[20] William H. McRaven, *Spec Ops, Case Studies in Special Operations Warfare: Theory and Practice* (New York: Random House, 1995), 4.

[21] William D. Bryant, "Cyberspace Superiority: A Conceptual Model," *Air & Space Power Journal* 27, no. 6 (November–December 2013), 25, available at <www.airuniversity.af.mil/Portals/10/ASPJ/jthenals/Volume-27_Issue-6/F-Bryant.pdf>.

[22] *Joint Operating Environment (JOE 2035): The Joint Force in a Contested and Disordered World* (Washington, DC: The Joint Staff, July 14, 2016), 36.

[23] *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (Fort Meade, MD: U.S. Cyber Command, 2018), 4.

[24] Air Force Doctrine Document (AFDD) 3-12, *Cyber Operations* (Washington, DC: Headquarters Department of the Air Force, July 15, 2010, incorporating Change 1, November 30, 2011), 50.

[25] McRaven, *Spec Ops, Case Studies in Special Operations Warfare*, 4. Emphases by authors.

[26] AFDD 3-12, 50.

[27] John B. Sheldon, "Deciphering Cyberpower: Strategic Purposes in Peace and War," *Strategic Studies Quarterly* (Summer 2011), 95–112.

[28] JP 5-0, *Joint Planning* (Washington, DC: The Joint Staff, 2017), III-2.

[29] *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 2011), 3.

[30] Gregory Wilson, "The Mystic Diamond: Applying the Diamond Model of Counterinsurgency in the Philippines," in *Gangs and Guerrillas: Ideas from Counterinsurgency and Counterterrorism*, ed. Michael Freeman and Hy Rothstein (Monterey, CA: Naval Postgraduate School, April 2014), 15. To gain a better understanding of the Diamond Model, see Gregory Wilson, "Anatomy of a Successful COIN Operation: OEF-Philippines and the Indirect Approach," *Military Review*, November–December 2006.

[31] United Nations Educational, Scientific, and Cultural Organization, "Concept of Governance," International Bureau of Education, available at <www.ibe.unesco.org/en/geqaf/technical-notes/concept-governance>. Emphases by authors.

[32] Ibid.

[33] *Achieve and Maintain Cyberspace Superiority*, 2, 7.