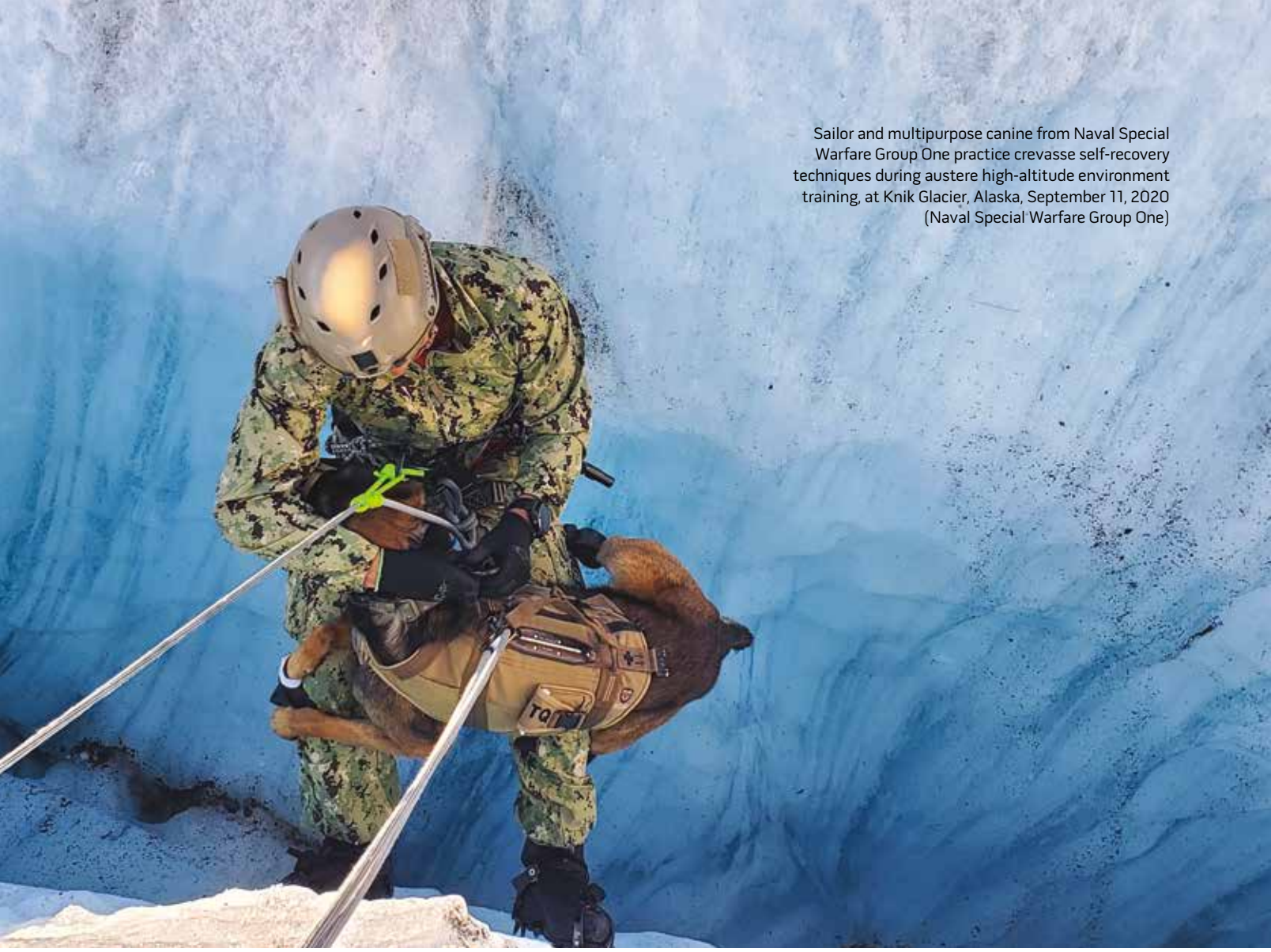


Sailor and multipurpose canine from Naval Special Warfare Group One practice crevasse self-recovery techniques during austere high-altitude environment training, at Knik Glacier, Alaska, September 11, 2020 (Naval Special Warfare Group One)

The Evolution of Special Operations as a Model for Information Forces

By Christopher E. Paul and Michael Schwille

U.S. special operations forces (SOF) writhed from perennial neglect before a dedicated combatant command—U.S. Special Operations Command (USSOCOM)—was created, an assistant secretary was appointed, and major force program funding was allocated. This article draws an analogy between historical SOF and contemporary information forces and suggests that the history and evolution of SOF could serve as a possible model and provide cautionary lessons for the future development of information forces.

Information and the information environment are ascendant in Department of Defense (DOD) concepts and conversations. There has been a great deal of productive thinking related to the

Christopher E. Paul is a Senior Social Scientist at RAND. Michael Schwille is a Senior Policy Analyst at RAND.

information environment over the past few years. Significant steps have included the publication of the *Department of Defense Strategy for Operations in the Information Environment* and the *Joint Concept for Operating in the Information Environment* (JCOIE), as well as the addition of information as a joint function—alongside command and control, intelligence, fires, movement and maneuver, protection, and sustainment.[1] Signed on July 25, 2018, the JCOIE represents important progress. It documents 17 required capabilities across 4 broad areas:

- characterize and assess the informational, human, and physical aspects of the security environment
- formulate options that integrate physical and informational power
- execute and modify those options
- institutionalize the integration of physical and informational power.

The JCOIE and the associated capabilities-based assessment have identified gaps in joint force capabilities, practices, and processes available to meet those requirements with the goal of identifying solutions. This effort established a need for more robust information-focused capabilities to support operation planning and the ability to command, control, oversee, and modify operations as they are executed and to leverage and employ informational power as part of operations. Meeting these needs will require the further growth and development of information forces (as pre-USSOCOM SOF needed to grow and receive more focused advocacy and funding in order to meet requirements).

But what do we mean by *information forces*? Information forces, at the very least, include those who contribute to understanding the human and informational aspects of operations, those who plan based on that understanding, and those who generate informational power. (The JCOIE describes *informational power* as the ability to leverage information to shape perceptions, attitudes, and other elements that drive desired behavior and the course of events.) Information forces might also include those who operate and maintain the DOD information network and knowledge management specialists. The information joint function also explicitly encompasses the management of information. Leaving aside information management and the inherent informational aspects of all military activities, information forces would comprise the existing capabilities of the planners and integrators of information operations (IO), the information-related capabilities (IRCs), and the portion of the intelligence apparatus dedicated to supporting efforts. The IRCs include a traditional core of electronic warfare, military information support operations (formerly psychological operations, whose personnel still self-identify as psychological operations), cyber operations, military deception, and operations security. More expansive lists of IRCs also include public affairs, civil affairs, combat camera, information assurance, counterintelligence, special technical operations, and, occasionally, a few others.

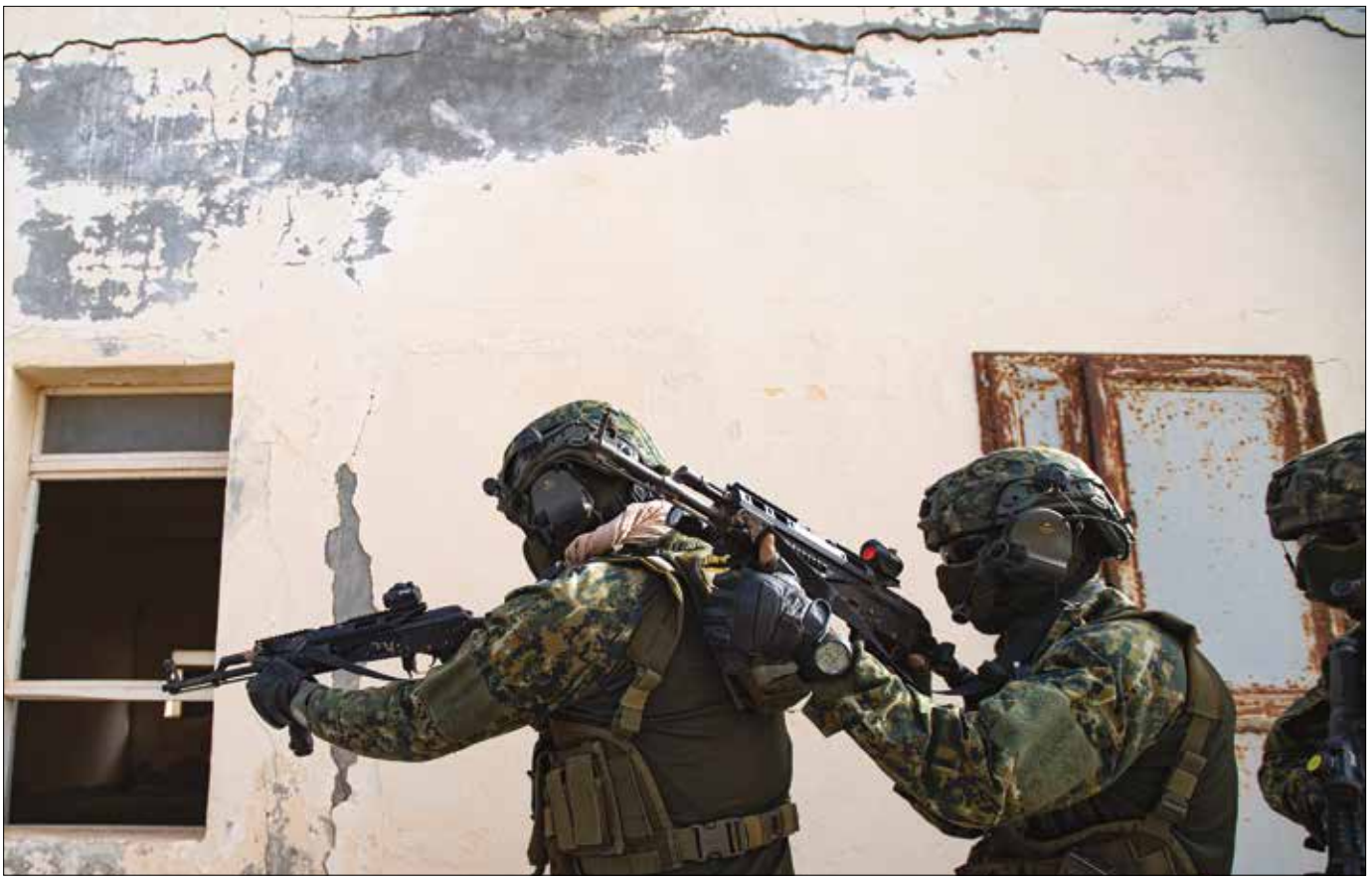
Many of these capabilities have been part of the joint force in one form or another for quite some time. Like SOF, what we now call *military information support operations* can trace its roots back to the Revolutionary War. Those early influence efforts involved colonial forces tying strips of paper containing promises of money, food, land, and freedom to rocks and throwing them at British forces to elicit their surrender.[2] Electronic warfare dates back to World War II, and the United States has had airborne jamming capability since at least the Korean War. Deception and operations security are tactics as old as warfare itself, but they lack force structure in the current joint force.

The IRCs have predominantly developed as niche capabilities in specialty areas and thus have evolved and operated independently of one another. Housed within the Services and often poorly understood by Service budget managers, many IRCs suffer from a lack of resources—and insufficient force structure is just one symptom.[3] Not only have some IRCs been historically undermanned, but many also still lack career fields, clear career progressions, or officer or enlisted military occupational specialties.[4] (Similarly, early SOF frequently saw their resources reprogrammed and these forces lacked clear career trajectories, with officers needing to rotate through conventional force postings in order to be promoted.) Further complicating matters, although we discuss these capabilities as part of information forces, personnel in the IRCs do not (yet) self-identify as belonging to broader information forces; instead, they identify with their capability, with their parent organization, or with their special position within the staff. Gathered together, cyber personnel, military information support operations personnel, public affairs officers, and foreign area specialists are more likely to focus on what differentiates them than on their commonalities.

IO emerged in joint doctrine in 1998 as a planning and integrating function seeking to coordinate the IRCs for a common purpose. Even with a doctrinally prescribed staff advocate, effectiveness fell short of what was envisioned. IRCs often lacked a coherent chain of command and reported to different headquarters elements. While the IO cell on a staff was meant to act as the nerve center for these forces, cells and working groups were often undermanned and not well integrated with their commands' standard processes and workflows.[5]

The 2003 *Information Operations Roadmap* sought to address many of these problems and called for IO to become a core competency in DOD, with a trained and capable career workforce to provide IO and related capabilities to the warfighter.[6] The *IO Roadmap* explicitly recognized isolated communities of specialists and relationships between capabilities, organization, education, career force, and analytic support as gaps. Overall, the "current state" as reported in the *IO Roadmap* indicated significant neglect of the development and maintenance of information forces. The state of affairs has improved marginally in many of the areas emphasized in 2003, but significant gaps persist today.[7]

With limited career fields, information forces remain undermanned, scattered across different stovepipes, poorly understood among commanders and staffs,



Guinean special forces soldiers conduct close quarters battle training in abandoned hotel during U.S. Africa Command's annual special operations forces exercise Flintlock 20, in Nouakchott, Mauritania, February 18, 2020 (U.S. Navy/Evan Parker)

and struggling to operate in harmony with each other. Wargames and exercises routinely ignore or underutilize IO and the IRCs—a product of the challenge of effectively simulating the information environment.[8] This has led to a reduced emphasis on IRCs in actual operations, as they have not been demonstrated to be important during training and rehearsals.

At one time, SOF suffered from many of the same challenges and shortfalls, but SOF are now effectively unified, institutionalized, funded, and supported with high-level advocacy. We believe that the ingredients that enabled SOF to grow from a precarious entity to a robust one are a good analogy and offer a possible template for future information forces.[9] The use of historical analogy in policymaking is unavoidable but can be somewhat perilous methodologically; cases that are insufficiently similar can lead to invalid generalizations.[10]

With that said, the two situations under consideration (historical SOF and contemporary information forces) have numerous similarities and appear to be ripe for analogy. The logic of analogy has face validity—the steps taken to reform SOF worked for its circumstances, and to the extent that the situation faced by SOF is similar to the situation faced by information forces, similar steps should work here, too.

Evolution of SOF and the Creation of USSOCOM

Elite commandos have always been a part of U.S. forces. The use of special forces dates back to the Revolutionary War, and modern U.S. SOF can directly trace their lineage to various World War II–era organizations. Despite this long history and many storied successes, SOF were repeatedly subject to postwar cutbacks and an accompanying deterioration of capabilities. This trend reflected tensions between SOF and conventional forces and what Susan Marquis described as the "precarious value" status of SOF:

> *Goals or missions within an organization . . . are in conflict with, or in danger of being overwhelmed by, the primary goals or missions of the organization. Precarious values may be at risk because of a lack of interest by the organizational leadership or because they are in conflict with the primary organizational culture, or sense of mission, of the institution.*[11]

After heavy employment in Vietnam, SOF were once again allowed to decay, limping into the 1980s. SOF struggled when employed due to ambiguous command relationships, ad hoc command and control relationships, and poor integration with conventional forces in planning (similar to the plight of information forces in the current era). Several high-profile failures highlighted these shortcomings and demonstrated institutional problems in how the Services supported SOF—making improvement unlikely. Most glaringly, the Services routinely budgeted for investment in

SOF or SOF equipment but would then usually revise or eliminate those budget lines to free up resources for Service priorities. This led to an acrimonious reform process that involved Congress imposing a new structure for the advocacy and support of SOF: USSOCOM and the Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict (ASD SO/LIC).[12] Congress also gave SOF access to dedicated funding through Major Force Program (MFP)–11 for SOF-peculiar equipment.

Congress had to impose these changes. The need for SOF reform had been apparent for some time and was highlighted by the 1981 disaster of *Desert One* in the Iranian desert that forced Operation *Rice Bowl* to abort instead of attempting the rescue of American hostages at the Embassy in Tehran, and by high SOF casualties in Grenada in 1983, where conventional force leaders misused SOF as light infantry.[13] These repeated disasters served to catalyze and sustain congressional attention. Congress repeatedly encouraged reform and change, writing directives and memos, and programming funding for SOF requirements by which were then repeatedly reprogrammed by the Services. By 1986, it became clear to congressional SOF advocates that sufficient reform would not come from inside DOD. In 1986, advocates in both the House and the Senate pushed through legislation, the Nunn-Cohen Amendment, that called for the establishment of a four-star SOF combatant command, an ASD, and a new Major Force Program.[14] This was the first time that Congress had mandated the creation of a military command. Further legislation in 1987, 1988, and 1989 proved necessary to force DOD to fully implement the reforms.

The creation of USSOCOM placed all SOF under one command, and the benefits were numerous. It aligned SOF force generation, training, and employment under a single command and provided flexible control options for SOF elements during operations. It opened SOF-distinct career paths and eliminated the need for personnel to return to the conventional forces to meet requirements for command billets. It ensured that SOF were commanded by headquarters elements that understood their capabilities and that forces were employed to maximum effect. The end point of the analogy would serve: All these things would also clearly benefit future information forces.

The creation of ASD SO/LIC explicitly provided high-level representation and advocacy for SOF. Congress demanded the creation of this position to defend resourcing, coordinate activities, and represent SOF interests.[15] ASD SO/LIC supports USSOCOM in much the same way as the various Service secretaries support their respective organizations.

The final ingredient in the transformation of SOF from precarious organization to enduring institution was the creation of MFP-11. MFPs are a group of program elements and the necessary resources to ensure successful completion of a mission, objective, or plan.[16] Primary funding for SOF comes from two MFPs: MFP-2 is for general purpose forces, and MFP-11 is specific to SOF. USSOCOM is able to tap these two funding streams because of its distinctive structure: It contains four separate Service components, and each Service is responsible for "Service-common" administration, training, personnel, and equipment. Items that are Service-funded include initial training, basic qualification training, pay, entitlements, officer and Service professional military education, tuition assistance, housing, family services, and access to on-base dining and fitness facilities.[17] In addition to what is funded through the Services, MFP-11 gives SOF the ability to acquire particular equipment for missions. This equipment is distinct from the standard equipment used by general purpose forces and often has different requirements and needs. The equipment can be altered Service-common equipment, equipment designed especially for SOF, or rapidly acquired commercial equipment fulfilling a specific capability requirement. The creation of MFP-11 was a significant change in that it allowed the SOF community to control the resources to obtain these items for missions. SOF no longer had to appeal to the Services and fight for priority within Service budgets every time a new requirement was generated. MFP-11 also provided resources to conduct SOF-specific research and development, something that the Services would routinely repurpose for other priorities during the period in which SOF languished. Today's information forces suffer similar challenges related to funding, with the Services able to reprioritize, deprioritize, or reprogram resources provisionally allocated for IRCs.

In short, the creation of USSOCOM gave SOF an institutional home, tasked these forces with a clear mission, increased their ability to plan and deploy worldwide, provided a coherent chain of command, provided a high-level advocate in the form of the ASD SO/LIC, and guaranteed access to dedicated funding through MFP-11.

Lessons from SOF Evolution

Information forces are *precarious values* in their current state in the same way that pre-USSOCOM SOF were. In learning from this analogy, what can the successful evolution of SOF tell us as we consider the future of information forces? Does the path that led to modern SOF suggest a possible model for future information forces? One of the key insights from the history of SOF is the value of a unified organizational and institutional home. The creation of USSOCOM placed all SOF under one command, which elevated the mission of SOF, centralized the management of SOF careers and training, and provided a clear chain of command for all SOF. To be successful, information forces will need a similar unified organizational home. Whether that should be a new four-star command such as USSOCOM or an existing command that is expanded and rebranded, such as U.S. Cyber Command, remains an open question. Recent discussion about restructuring U.S. Army Cyber Command to become U.S. Army Information Warfare Command might be an example of a Service-level solution, depending on what that actually comes to look like.[18]

Special Tactics Airmen assigned to 26th Special Tactics Squadron post security during full mission profile at Melrose Air Force Range, New Mexico, March 11, 2020 (U.S. Air Force/Maxwell Daigle)

Another essential element of the SOF model is the high-level advocate embodied in ASD SO/LIC, who serves the SOF community in much the same way as the Service secretaries work for their respective organizations—defending resources, coordinating activities, and representing interests. If information forces are to fulfill the requirements laid out in the JCOIE, they will need a similar high-level advocate and defender. In fact, Congress has already demanded something like this role in the 2019 National Defense Authorization Act, Section 1631(a), which calls for the designation of a Principal Information Operations Advisor (PIOA) with a host of responsibilities related to policy and oversight for operations in the information environment. Though a final decision about the level of this PIOA has not been made at the time of this writing, it is clear that this position will be the highest level advocate and proponent for information forces and operations in the information environment to date. Moreover, unlike previous senior advisors (such as the "designated senior official" called for in the 2018 National Defense Authorization Act), the PIOA will be a dedicated full-time position, not an official with multiple portfolios of responsibility wherein information is a secondary (or tertiary) responsibility. Part of the reason that ASD SO/LIC is an effective advocate for SOF is that the office's advocacy role is a central and primary responsibility.

The history of SOF suggests that an organizational home and a senior advocate alone would be insufficient for information forces at this stage of development. The final element in the successful SOF model was a secure resourcing stream as embodied in MFP-11. As a combatant command, USSOCOM has access to resources through general funding mechanisms (such as operations and maintenance, military construction, and research and development), as well as through its own unique line of funding. Taking this as a possible model for information forces, the creation of an MFP-12 or some other enduring and designated funding stream would ensure that the resources required to equip and enable information forces would actually be provided and not reprioritized by other stakeholders, as happened repeatedly with SOF investment under the Services and as seen to some extent for the IRCs under the control of USSOCOM—that is, military information support operations and civil affairs—and the Services.

While the creation of USSOCOM, ASD SO/LIC, and MFP-11 eliminated many of the perennial challenges plaguing early SOF, some remain. Specifically, because SOF are segregated in their training and resourcing and have their own

chain of command, occasionally special operations are still not well integrated with other operations. Information forces have also faced this challenge, with information and information-related capabilities frequently excluded from consideration in planning and sometimes being invited to "sprinkle some of that IO stuff" on already completed plans.[19] More robust information forces should positively contribute to integration by being more capable, better understood, and having more vigorous advocacy. However, information forces (and commanders) will need to guard against their exclusion and inappropriate expectations that they will operate in the information environment somehow separate from the rest of the force and the rest of the operating environment.

Without some kind of change, the goals identified in the 2003 *Information Operations Roadmap*, the 2016 *Strategy for Operations in the Information Environment*, and the 2018 JCOIE will continue to be an uphill struggle. For SOF, the necessary reforms required vigorous and repeated intervention by Congress. While congressional attention and input addressing the reform of capabilities and organization related to the information environment is building, it has by no means yet reached the level of congressional pressure that proved necessary to achieve SOF reform. Hopefully, resistance to reform within DOD will be less for information forces than for historical SOF, and the more modest level of congressional pressure currently present will prove sufficient.

If information forces are going to be available to meet growing demands and compete with Russia and China in the information environment, they must be developed and institutionalized in a way that protects them from being precarious values. SOF were able to escape their status as precarious values, and an analogy with the evolution of SOF offers a possible model for the future of information forces. SOF succeeded with a new organizational home, high-level advocacy, and secure funding. The analogy between SOF and information forces suggests that these three elements would be extremely beneficial in overcoming the challenges now faced by information forces. We would do well to learn these lessons through example and analogy rather than experience to avoid repeating the failures of pre-USSOCOM SOF. **JFQ**

Notes

[1] See the three articles discussing information as a joint function in *Joint Force Quarterly* 89 (2nd Quarter 2018): Alexus G. Grynkewich, "Introducing Information as a Joint Function," available at <http://ndupress.ndu.edu/Media/News/News-Article-View/Article/1490517/introducing-information-as-a-joint-function>; Scott K. Thompson and Christopher E. Paul, "Paradigm Change: Operational Art and the Information Joint Function," available at <http://ndupress.ndu.edu/Media/News/News-Article-View/Article/1490645/paradigm-change-operational-art-and-the-information-joint-function>; and Gregory C. Radabaugh, "The Practical Implications of Information as a Joint Function," available at <http://ndupress.ndu.edu/Media/News/News-Article-View/Article/1490782/the-practical-implications-of-information-as-a-joint-function>.

[2] William Daugherty and Morris Janowitz, *A Psychological Warfare Casebook* (Baltimore: The Johns Hopkins University Press, 1958).

[3] Christopher J. Lamb, *Review of Psychological Operations Lessons Learned from Recent Operational Experience* (Washington, DC: NDU Press, September 2005).

[4] Joseph L. Cox, *Information Operations in Operations Enduring Freedom and Iraqi Freedom—What Went Wrong?* (Fort Leavenworth, KS: School of Advanced Military Studies, 2006), available at <https://fas.org/irp/eprint/cox.pdf>.

[5] Dennis M. Murphy, *Talking the Talk: Why Warfighters Don't Understand Information Operations*, Issue Paper, Vol. 4-09 (Carlisle Barracks, PA: Center for Strategic Leadership, May 2009).

[6] *Information Operations Roadmap* (Washington, DC: Department of Defense, October 30, 2003).

[7] Richard B. Davenport, "The Need for an Innovative Joint Psychological Warfare Force Structure," *Joint Force Quarterly* 88 (1st Quarter 2018), 64–69, available at <https://ndupress.ndu.edu/Publications/Article/1412317/the-need-for-an-innovative-joint-psychological-warfare-force-structure/>.

[8] James R. McGrath, "Twenty-First Century Information Warfare and the Third Offset Strategy," *Joint Force Quarterly* 82 (3rd Quarter 2016), 16–23, available at <https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-82/Article/793229/twenty-first-century-information-warfare-and-the-third-offset-strategy/>.

[9] For an example of a similar application of the analogy of the evolution of special operations forces with future cyber forces, see Christopher E. Paul, Isaac R. Porche III, and Elliot Axelband, *The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces* (Santa Monica, CA: RAND, 2014), available at <www.rand.org/pubs/research_reports/RR780.html>.

[10] See, for example, the concerns raised in Yuen Foong Khong, *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965* (Princeton: Princeton University Press, 1992).

[11] Susan L. Marquis, *Unconventional Warfare: Rebuilding U.S. Special Operations Forces* (Washington, DC: Brookings Institution Press, 1997), 7.

[12] Rod Lenahan, *Crippled Eagle: A Historical Perspective of U.S. Special Operations, 1976–1996* (Charleston, SC: Narwhal Press, 1998).

[13] Marquis, *Unconventional Warfare*; Lenahan, *Crippled Eagle*.

[14] U.S. Special Operations Command (USSOCOM), *History*, 6th ed. (MacDill AFB, FL: USSOCOM, 2008).

[15] Linda Robinson, Austin Long, Kimberly Jackson, and Rebeca Orrie, *Improving the Understanding of Special Operations: A Case History Analysis* (Santa Monica, CA: RAND, 2018), available at <www.rand.org/pubs/research_reports/RR2026.html>.

[16] Defense Acquisition University, "Defense Acquisition Glossary," available at <www.dau.edu/glossary/Pages/Glossary.aspx>.

[17] Fran Machina, *U.S. Special Operations Command Resourcing Special Operations* (Alexandria, VA: American Society of Military Comptrollers Professional Development Institute, May 30, 2014).

[18] Kimberly Underwood, "Army Cyber to Become an Information Warfare Command," *Signal*, March 14, 2019, available at <www.afcea.org/content/army-cyber-become-information-warfare-command>.

[19] Murphy, *Talking the Talk*, 2.