Technology Adoption in Unconventional Warfare

Sean W. Pascoli
Mark Grzegorzewski

ABSTRACT

As US Special Operations Command (USSOCOM) rebalances its primary focus, shifting from Violent Extremist Organizations (VEOs) to competition with Russia and China, there must be a greater emphasis on integrating cyberspace capabilities into the Unconventional Warfare (UW) doctrine. Section 1202 of the National Defense Authorization Act for Fiscal Year (FY) 2018 designates USSOCOM as the lead for irregular warfare,[1] empowering Special Operations Forces (SOF) to leverage select irregular forces, resourced under specific legal authorities to live off the land in support of irregular warfare missions. Combatant Commands retain operational command and control despite this designation. As a recommendation on how the US should employ non-traditional forces, this article shows how nation-states like China, North Korea (DPRK), Iran, and Russia use cyber proxies to conduct combined operations. It then considers how SOF can add an asymmetric technique to unconventional warfare by using cyber-capable irregular forces at the tactical level to serve as force multipliers. Finally, the USSOCOM Resistance Operations Concept (ROC) will be expanded to demonstrate how to better engage cyber proxies within UW.

Keywords: unconventional warfare, proxies, special operations forces, Russia, China

PURPOSE

Technology adoption is more than just the employment of a particular piece of hardware, like an iPhone or a new operating system, it can also entail a new way of thinking. US Special Operations Command (USSOCOM) is in the process of strategically rebalancing and will include both Violent Extremist Organizations (VEOs) and Great Power Competition (GPC) after two decades of near-exclusive focus on counterterrorism. This strategic rebalance requires a detailed review of resources, training, and

Sean Pascoli, a member of the Marine Corps Forces Cyberspace Command (MARFORCYBER) Cyber Operations-Integrated Planning Element (CO-IPE) at United Special Operations Command (USSOCOM), serves as the Cyber Exercise Branch Chief in the J3-Joint Collective Training Branch. He retired after twenty-four years in the Marine Corps and transitioned into a second career as a cyber planner. A University of Chicago graduate (1990) with a BA in Political Science and two master's degrees from the University of South Florida (USF) in Cyber Intelligence and Cybercrime, Mr. Pascoli also holds graduate certificates from USF in Information Assurance and Digital Forensics. His area of academic focus is the nation-state use of cyber surrogates and proxies.

doctrine as a result of the national security paradigm returning to nation-states and deterring near-peer adversaries. As a result, the US Government (USG) now employs the full-spectrum of information operations to compete in the gray space between peace and armed conflict. To adapt and compete, USSOCOM must become more versatile and resourceful in applying limited assets and resources to this fight. Pointing to the need to adapt, the Theater Special Operations Command Manning Review found that a core USSOCOM mission that should be re-invigorated and implemented in several Geographic Combatant Command Campaign plans is Unconventional Warfare (UW).[2]

The Joint Staff defines UW as "activities conducted to enable a resistance movement or insurgency to coerce, disrupt or overthrow a government or occupying power by operating through or with an underground, auxiliary and guerrilla force in a denied area."[3] A critical, detailed USSOCOM planning document for applying UW is the Resistance Operating Concept, which is a reflection on the past in that it addresses the need for countries to resist against occupation, just as Eastern Europe did during the Cold War.

This new breed of Russian threat, hybrid and unconventional, violent and non-violent, has forced USSOCOM to look for a different approach in this space since the doctrines of combined arms maneuver, counterterrorism, and counterinsurgency may no longer apply.[4] The Kremlin's view of warfare views the human mind as the key terrain which means the next war will be won in the information domain by psychological warfare.[5] To win here, Russia will deploy its less robust conventional forces only when absolutely necessary.[6] Instead, Russia will focus its resources by forcing its adversary's military and citizens to respond to the attacker and expend its own resources.[7] In response, USSOCOM's answer to this "new" Russian way of war is the Resistance Operations Concept (ROC); a new interpretation of the centuries-old theory of UW.[8]

Dr. Mark Grzegorzewski, a Resident Senior Fellow at Joint Special Operations University (JSOU) currently focused on researching cyberspace operations and artificial intelligence (AI). He is recently published in *Special Operations Journal* on "Demystifying Artificial Intelligence through DoD Education" and also "Supporting Resistance Movements in Cyberspace." He also has a chapter in an edited volume titled "Russian Cyber Operations: The Relationship Between The State And Cyber Criminals." He created JSOU's *Quick Look* series with a publication on AI, and a forthcoming *Quick Look* piece on Cryptocurrency. Dr. Grzegorzewski holds a Ph.D., M.A., and B.A. in Political Science from the University of South Florida, along with a graduate certificate in Globalization Studies.

ROC Needs More "Cyber"

The Resistance Operating Concept was established to support the Eastern European members of the North Atlantic Treaty Organization (NATO): Estonia, Latvia, and Lithuania. These countries are attempting to withstand Russia's increasing aggression to reclaim its former territories: it uses various methods of hybrid warfare, combined with its advantage of interior lines to quickly seize the Baltic countries. These three countries are vulnerable as they are part of the former Soviet Union. Short of the ability to resist, these Eastern European states are threatened by Russia's operational dexterity and the lack of a large Europe-based US conventional force to credibly deter aggression.[9] As Estonia, Latvia, and Lithuania lack a readily available counter to Russia's aggression, the Resistance Operating Concept supports them by addressing the inadequacies of the conventional military, national defense planning and preparation by supporting a Total Defense model where the citizenry is the primary actor instead of the government.[10] Of relevance for SOF to consider, perhaps given that the citizen is at the center of this model where they must always be prepared for invasion, the Resistance Operating Concept perhaps should be known as the Persistence Operating Concept.

Total Defense is ideally suited for countries who share a border with hegemonic powers, and "includes all the necessary activities to prepare a nation for conflict in defense of its independence, sovereignty, and territorial integrity; and consists of both civil and military defense."[11] It encompasses all societal functions needed to mobilize the support necessary to defend the nation and its territorial integrity against armed attack.[12] USSOCOM's support to Baltic resistance would primarily consist of Special Forces Operational Detachment-Alpha, or A-Teams,[13] executing UW campaigns by employing proxies to enable the resistance in a contested area.

But the current ROC, insofar as deployable UW cyberspace tools, is virtually non-existent in SOF A-Teams, due to several reasons ranging from capabilities to capacity, as well as risk aversion and ignorance of authorities. Currently, A-Teams are insufficiently prepared to conduct cyber operations. To task an A-team with such a mission would be a significant leap forward, but would also be very dangerous. Yet, far too often authorities are cited to excuse inaction in cyberspace. The 2018 National Cyber Strategy,[14] the 2018 National Defense Authorization Act (NDAA), and the 2021 NDAA Section 1299, Functional Center for Security Studies in Irregular Warfare)[15] all point to a maturation of public cyber policy relating to SOF forces. This flood of newly published unclassified national-level strategy and policy documents empowers SOF to act within its mission set.

This deficiency can be mitigated by taking a page out of Russia and China's playbooks and employing cyber proxies that can effectively impose costs on the adversary.[16] Cyber proxies serve as intermediaries that conduct or directly contribute to an offensive cyberspace action that is either actively or passively enabled by a beneficiary.[17] Fiscal authority exists to leverage select foreign forces in support of irregular SOF warfare missions, and cyber forces can be employed by A-Team forces.

Cyber Proxies and SOF

One DoD concern may be that cyber-capable irregular forces can employ unsanctioned cyber operations that pose an unacceptable risk for senior leaders. Nothing prevents the use of kinetic capabilities that cause serious physical damage, but some DoD senior leaders still see cyberspace operations as a bridge too far in UW campaigns. The DoD must overcome this unfounded fear that cyberspace operations should be reserved for existential, strategic threats against the US so that these capabilities can be normalized in all DoD operations that have signed Execute Orders. Many nations, including the US' biggest adversaries—China, Russia, Iran, and North Korea—have normalized the use of cyber proxies with great success.[18] As such, SOF should be wargaming these new tradecraft methods and techniques to prepare our Forces to conduct combined operations against our adversaries in the multiple domains where they now confront us.

Including cyber-capable irregular forces as integral to SOF principles of support to UW is not an intellectually heavy lift and has the second- and third-order effects of protecting the US from its adversary's ability to conduct cyber-attacks by causing them to focus inward on domestic security, and lose trust in their cyber proxies, thereby allowing the US to maintain its technological edge in the cyber domain.[19] The effectiveness of an insurgency is well known to the DoD, especially SOF, which for over two decades has fought to overcome various insurgencies in Afghanistan and Iraq—insurgencies that massively drained US human and financial resources. Embedding a cyber component or line of operation within the ROC would result in the cyber proxy serving as a force multiplier in any UW campaign. For example, supporting cyberspace UW/ROC by enabling infrastructure and networks, used by hacktivists and other wired individuals in an occupied Baltic country, would force Russia to look inward and drain its capabilities and capacity to fight a digitally enabled insurgency. By enabling infrastructure and networks, they could be used for either commercial or military purposes so only the intention of use changes, not the infrastructure. Such distractions would erode the adversary's ability to conduct external cyberspace operations or otherwise attack American targets. A cyber-enabled UW campaign in Eastern European countries would enable SOF cyber proxies to enhance the overall UW/ROC campaign plan.

It's High Time to Implement Cyber UW

Cyber-enabled UW is not a new concept. Among the Special Forces practitioners who have published on the topic, the foremost advocate has been COL(Ret.) Patrick Duggan. He was the first to propose sending UW pilot teams into cyberspace.[20] Duggan envisioned these teams as influencing the environment by targeting social media networks, deploying UW pilot teams that essentially lived off the land by employing dual-use commercial technologies, indigenous equipment, and local networks of influence. Once the environmental conditions were established locally, these UW pilot teams could influence social media's gray and dark networks from their home base. Duggan correctly notes the ability of UW pilot teams is constrained only by their authorities. This remains a hurdle, even though some authorization has in recent years been pushed down to the operational levels, as some Commanders remain reticent to delegate as advocated by Duggan, given the unintended operational effects that sometimes materialize with social media operations.

Duggan also urges the use of cyberspace capabilities to be employed in Special Warfare (foreign internal defense, UW, and counterinsurgency).[21] Special Forces (SF) in Duggan's view could exploit cyberspace to identify, assess, and evaluate resistance leaders and capabilities, and otherwise better understand the environment in which they are operating. Once armed with the proper infrastructure and an operational mission, these Cyber UW pilot teams could also deploy to the physical environment and further nurture relations with resistance forces.

Duggan persists in arguing for man-machine teaming in UW, urging the DoD to keep pace with its competitors and increase the use of emerging technology, including 3-D printing during operations.[22] He also promotes cyber-enabled UW financial warfare, using cyberspace to distort the price of goods, and SOF's ability to compromise the confidentiality, integrity, and availability of open adversary networks using cyber tools. One challenge Duggan briefly addresses without elaboration is the potential effect of man-machine teaming micromanaging tactical actions from operational level commands in the same way that the telegram was used to micromanage during World War I. This remains a valid concern today and requires continued attention to balance between a Commander's need to know with operational flexibility.

Duggan also argues the DoD must recognize that the character of conflict is changing, and SOF is perfectly suited to operate in cyberspace given that cyber-warfare is essentially human-warfare and SOF specializes in the human domain.[23] Employing SOF's light footprint and unconventional mindset in the cyber domain provides the DoD with another tool in its deterrence strategy. As such, SOF must continue to understand an adversary's environment, including factors that drive its behavior and each society's relationship with information. SOF can then exploit these insights and thereby divert the adversary inward.

Agreeing with Duggan's arguments, Benjamin Brown in 2018 called for the creation of a "CYBERSOC" (Cyber Special Operations Command), nested within USSOCOM, arguing the need for cyber operators to support special operations.[24] Thus, CYBERSOC would support the twelve special operations core activities and conduct its own missions with cyber as the primary line of effort. Brown and Duggan agree that cyberspace overlaps with the human domain, making SOF ideally suited to take on the cyberspace special operations mission set.

COL (Ret.) Brian Petit, another former US Army Special Forces practitioner, envisions a role for SOF in cyberspace via social media.[25] He sees social media and the way it can enable unconventional warfare an essential part of any UW campaign. The social media environment reflects reality in some ways and SOF can use this space to identify resistance potential and could conceivably support a resistance movement. This could include amplification of social media messages, providing communications equipment, creating social media accounts, and even influencing messaging. To Petit, SOF's role in social media should always be set to "on," whether gathering targeting data or shaping/suppressing information.

This discussion contributes to UW cyber literature by explaining how a new actor, cyber-capable irregular forces, could work with UW forces, and builds upon the ideas from the Resistance Operating Concept. Concepts of resistance movements and unconventional forces are imperfect fits, and only one of many types of social movement that unconventional warfare supports and leverages. Yet the insertion of more cyberspace capabilities into UW writ large will give SOF greater impact in navigating revolutionary and insurgent social movements.

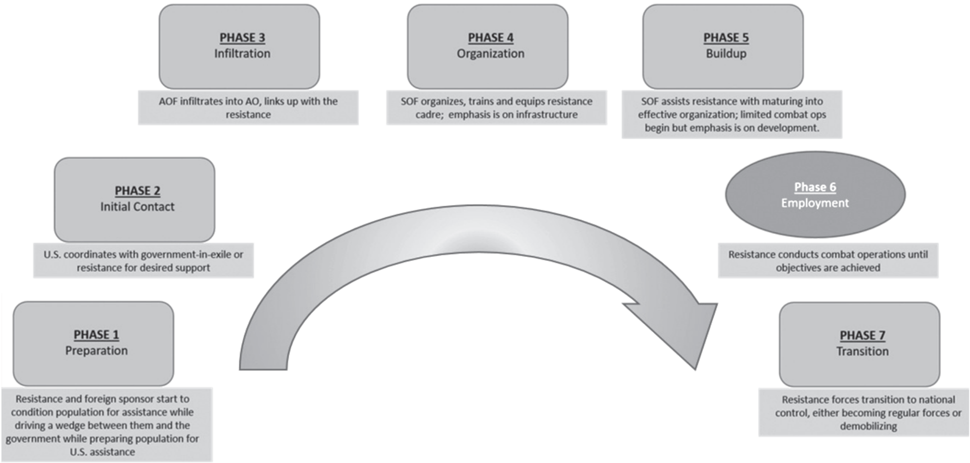
Cyber-Capable Irregular Forces

As Russia seeks to gain influence in cyberspace, the DoD has been directed to engage in cyberspace more robustly below the level of armed conflict. Cyber proxies mitigate attribution concerns and allow DoD to execute offensive cyberspace operations. For some time now, Russia, China, Iran, and North Korea have conducted joint operations with cybercriminal elements that mask their nation-state activities, and countering these activities in-kind it would be a force multiplier for UW campaigns.[26],[27]

Their label as criminals of course poses challenges for DoD to leverage cybercriminals to counter enemy behavior, without attribution. That said, the definition of crime varies widely in different countries. For example, individuals pushing back against a corrupt regime or exposing wrongdoing could be labeled as criminals. Therefore, working with these cyber-capable irregular forces would serve as an agile, responsive UW force that could effectively degrade threat actions below the level of armed conflict. By identifying, assessing, and evaluating these forces during the preparation phase, SOF-enabled infrastructure and networks in a UW cyberspace campaign could help counter Russian aggression in Eastern Europe.

Where Should Cyber Fit?

The seven phases of SOF support to UW (see Figure below) serve as an intellectual framework for UW cyber activities and operations and are easily adaptable to the cyber domain and a cyber-enabled ROC.[28] These phases will not always run sequentially. Indeed, operators will move in all directions among the UW phases and sometimes even operate multiple phases simultaneously.



AOF infiltrates into AO, links up with the resistance

SOF organizes, trains and equips resistance cadre; emphasis is on infrastructure

SOF assists resistance with maturing into effective organization; limited combat ops begin but emphasis is on development.

U.S. coordinates with government-in-exile or resistance for desired support

Resistance conducts combat operations until objectives are achieved

Resistance and foreign sponsor start to condition population for assistance while driving a wedge between them and the government while preparing population for U.S. assistance

Resistance forces transition to national control, either becoming regular forces or demobilizing

Figure 1. Seven Phases of Unconventional Warfare

1. Phase I Preparation

a. **Physical Domain:** Resistance and external sponsors conduct psychological preparation to unify the population against the occupier and prepare the population to accept US support.

b. **Cyber Domain:** Analyze online information environments; ask how the society influences and responds to social media; identify online opposition groups in target countries. Include hacktivists, peacefully opposed organizations, university computer clubs, and cybercriminals. Examine the online environment; identify risks to mission and threats to the occupying force (including leverageable dissidents within the occupying force). Determine (a) cyber-capable irregular force access to occupier's open networks, and (b) available open-source and living-off-the-land tools[29] for resistance force to leverage against the occupier.

2. **Phase II Initial Contact**
   a. **Physical Domain:** US agencies coordinate with allied governments-in-exile or resistance leaders for needed US support.

   b. **Cyber Domain:** Establish contact with hacktivist leaders and online elements through forums and chatrooms; demonstrate technical ability to support cause. Use clandestine methods and applications (i.e., virtual private network (VPN), the onion router (TOR), disposable e-mail accounts, etc.) to reach cyber-proficient opposition. Use overt methods and applications to reconnoiter networks connected to the Internet of Things.[30]

3. **Phase III: Infiltration**
   a. **Physical Domain:** SOF infiltrates into the operational area, establishes communications with its base, and contacts resistance organization.

   b. **Cyber Domain:** Phase II and III combine in the cyber domain since infiltration can be digital until trust is developed to enable contact in the physical domain. Infiltration is also an infrastructure-specific effort that maintains traffic anonymity into the area of operations and contacting hacktivist leadership. This phase may also include the introduction and coordination of the cyber proxy and the physical proxy, (if not one and the same). SOF and cyber-capable irregular force communication can be conducted via ad hoc wireless, meshed networks.[31]

4. **Phase IV: Organization**
   a. **Physical Domain:** SOF organizes, trains, and equips resistance cadre with an emphasis on developing infrastructure.

   b. **Cyber Domain:** Provide communication methods or forums for hacktivists to conduct Command & Control (C2) and receive guidance, capabilities, and training from SOF cyber, potentially including Force Protection (ForcePro) and use of open-source intelligence (OSINT) for targeting. SOF can transfer money to the cyber-capable irregular forces via an obscured ledger cryptocurrency that conceals the sponsor. SOF can also provide various 3-D printable designs that the cyber-capable irregular forces could employ and identify dual-use technologies.

5. **Phase V: Buildup**
   a. **Physical Domain:** SOF assists cadre expansion into an effective resistance organization; while emphasis is development, limited combat operations may be conducted.

   b. **Cyber Domain:** Provide offensive cyber capabilities training and limited system and target information to increase capability and capacity to achieve desired outcomes. Have proxy forces find open-source code, as well as code and tools from dark-net hacker marketplaces, for cyber-capable irregular force use. Work with cyber-capable irregular forces to produce both cyber effects and real-world effects. Create coordinated domain crossing effects for maximum effect.

6. **Phase VI: Employment**
   a. **Physical Domain:** UW forces conduct combat operations until linkup with conventional forces or end of hostilities.

   b. **Cyber Domain:** Hacktivists conduct offensive cyber operations until strategic goals below the level of armed conflict are achieved, or until the desired decrease in the target nation's external cyber operations is reduced to acceptable levels. These effects should be scalable and reversible. Observe cyber-capable irregular forces to prevent employing effects that could harm critical infrastructure or the private sector that could also harm the occupied population. Also, ensure that cyber-capable irregular forces' effects are not undermining government-in-exile's political objectives. Finally, cyber-capable irregular forces may display hacked or other compromising, occupying force information to influence the information domain.[32]

7. **Phase VII: Transition**
   a. **Physical Domain:** UW forces revert to national control, shifting to regular forces or demobilizing.

   b. **Cyber Domain:** The cyber proxy demobilizes and promotes national stability, ensuring the free information flow on the internet. Cyber-capable irregular forces restore cyber effects to the national government, retaining connectivity to infrastructure and networks. Preserve plausible deniability as to DoD affiliation, thereby (a) giving cyber-capable irregular forces and host nation government legitimacy with the population for home grown cyber operations, and (b) allowing the sponsoring government to employ similar tactics, techniques, and procedures elsewhere.

CONCLUSION

What is old is new again. UW, which had assumed a tertiary role in the US' counterterrorism fight, has returned with a vengeance. As the threat of Russian dominance hangs over Eastern European countries, resistance within the context of unconventional warfare has once again become relevant. Instead of blindly following lessons of the past, the US must use technology and cyberspace within UW to effectively combat today's threats. The new thinking we advocate includes employing cyber-capable irregular forces in the cyber domain by enabling infrastructure and networks against occupying forces. What matters when enabling infrastructure and networks is intentions, and how it is engaged. Thus, SOF must persist in this space 24/7. Non-cyber resistance forces are routinely armed with lethal weaponry. DoD's reluctance to engage cyber proxies must come to an end.

Until senior leaders' comfort level with cyberspace operations matches their comfort level with tactical nuclear weapons, amphibious assaults, and carpet bombing, US military forces will continue to operate with one hand tied behind their back. The US must increase efforts at developing, enabling, and maintaining infrastructure and networks to take full advantage of its Cyber Mission Teams and Cyber Operating Forces. Once this paradigm shifts and USSOCOM embraces the centrality of enabled infrastructure and networks, SOF will be much better positioned to compete more effectively with adversaries in the cyberspace domain, and, indeed, across domains. Until then, its technological edge in military cyberspace over near-peer competitors will continue to erode.

NOTES

1. Deputy Secretary of Defense, "Directive-type Memorandum (DTM)-18-005 - Authority for Support of Special Operations for Irregular Warfare (IW)," August 3, 2018, https://fas.org/irp/doddir/dod/dtm-18-005.pdf.
2. Hal Brands and Tim Nichols, "Special Operations Forces and Great-Power Competition in the 21st Century," American Enterprise Institute, August 2020, https://www.aei.org/wp-content/uploads/2020/08/Special-Operations-Forces-and-Great-Power-Competition-in-the-21st-Century.pdf.
3. Kevin Stringer and Glennis Napier, *Resistance Views: Essays on Unconventional Warfare and Small State Resistance, Tartu Resistance Seminar* (Tampa: JSOU Press, 2019), 66.
4. Nicu Popescu and Stanislav Secrieru, eds., *Hacks, Leaks and Disruption-Russian Cyber Strategies* (Paris: European Union, Institute for Security Studies, 2018).
5. Booz Allen Hamilton, *The Logic Behind Russian Military Cyber Operations* (Washington, DC: Booz Allen Hamilton, 2020).
6. Quentin Hodgson, Logan Ma, Krystyna Marcinek, and Karen Schwindt, *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace*, (Santa Monica, CA: RAND, 2019).
7. Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020).
8. Otto Fiala, *Resistance Operating Concept* (Tampa: JSOU Press, 2019).
9. Kevin Stringer and Glennis Napier, *Resistance Views: Essays on Unconventional Warfare and Small State Resistance, Tartu Resistance Seminar* (Tampa: JSOU Press, 2019).
10. Otto Fiala, *Resistance Operating Concept* (Tampa: JSOU Press, 2019).
11. Ibid.
12. Kevin Stringer and Glennis Napier, *Resistance Views: Essays on Unconventional Warfare and Small State Resistance, Tartu Resistance Seminar* (Tampa: JSOU Press, 2019).
13. There are six A detachments in each Special Forces company. A major or a senior captain leads the 12-man team. Second in command is a warrant officer. Two noncommissioned officers, or NCOs, are trained in each of the five SF functional areas: weapons, engineering and demolitions, medicine, communications, operations and intelligence, and comprise the remainder of the team. All team members are Special Forces qualified and cross-trained in different skills as well as being multilingual.
14. White House, "National Cyber Strategy," September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
15. 116th Congress, "SEC. 1299L. Functional Center for Security Studies in Irregular Warfare," *Small Wars Journal*, December 30, 2020, https://smallwarsjournal.com/blog/sec-1299l-functional-center-security-studies-irregular-warfare.
16. Tim Maurer, *Cyber Mercenaries* (Cambridge, UK: Cambridge University Press, 2018)
17. Ibid.
18. Quentin Hodgson, Logan Ma, Krystyna Marcinek, and Karen Schwindt, *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace* (Santa Monica, CA: RAND, 2019).
19. Tim Maurer, *Cyber Mercenaries* (Cambridge, UK: Cambridge University Press, 2018).
20. Patrick Duggan, "UW in Cyberspace," *Special Warfare* 27, no. 1 (2014): 68-70.
21. Patrick Duggan, "Strategic Development of Special Warfare in Cyberspace," *Joint Force Quarterly*, October 1, 2015, https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-79/Article/621123/strategic-development-of-special-warfare-in-cyberspace/.
22. Patrick Duggan, Man, Computer, and Special Warfare, *Small Wars Journal,* January 4, 2016, https://smallwarsjournal.com/jrnl/art/man-computer-and-special-warfare.
23. Patrick Duggan, Why Special Operations Forces in US Cyber-Warfare? *The Cyber Defense Review* 1, no. 2 (2016), 73-79.
24. Benjamin Brown, "Expanding the menu: The case for cybersoc," *Small Wars Journal*, January 5, 2018, https://smallwarsjournal.com/jrnl/art/expanding-menu-case-cybersoc#:~:text=The%20United%20States%20military%20should,U.S.%20interests%20and%20national%20security.
25. Brian Petit, Social Media and UW, Special Warfare 25, no. 2 (2012): 20-28.
26. Jonathan Lusthaus, *Industry of anonymity: Inside the business of cybercrime* (Cambridge, MA: Harvard University Press, 2018).
27. Mark Grzegorzewski, "Russian Cyber Operations: The Relationship between the State and Cybercriminals" in *Historical and legal aspects of cyber attacks on critical infrastructure*, edited by Denis Čaleta and James F. Powers (Ministry of Defense, Republic of Slovenia, Joint Special Operations University, and Institute for Corporative Security Studies, Ljubljana, Slovenia, 2020), 53-64.

NOTES

28. Kevin Stringer and Glennis Napier, *Resistance Views: Essays on Unconventional Warfare and Small State Resistance, Tartu Resistance Seminar (*Tampa: JSOU Press, 2019).
29. Living-off-the-land tools include those instruments that are low signature, low attribution, and low power.
30. David Kilcullen, "The Evolution of Unconventional Warfare," *Scandinavian Journal of Military Studies 2*, no. 1 (2019).
31. Patrick Duggan, "To Organize Cyber, Humanize the Design," *Small Wars Journal,* November 21, 2016, https://smallwarsjournal.com/jrnl/art/to-operationalize-cyber-humanize-the-design.
32. Megan K. McBride, Zack Gold, and Kasey Stricklin, "Social Media Bots: Implications for Special Operations Forces," Center for Naval Analysis, September 2020, https://www.cna.org/CNA_files/PDF/DRM-2020-U-028199-Final.pdf.