Kingston Consortium on International Security

Insights

December 2022 Volume 2, Issue 12

SOF Hyper-Connected and Hyper-Enabled Technology:

SOF's Strength or SOF's Achilles' Heel?

Col (Retired) Derek Jones
US Army, Special Forces

LTC (Retired) Dan Leaf
US Army, Special Forces

Technology has historically provided significant advantages for Special Operations Forces (SOF). The two decades after 9/11 witnessed the emergence of myriad technologies that enabled an unprecedented level of SOF operations against non-state actors, such as al Qaeda and the Islamic State. Today, as SOF transitions from the war on terrorism to great power competition (GPC) and potential future great power conflict, SOF is turning to technology once again as the main tool for maintaining its competitive advantage over near-peer threats. The primary technology-driven SOF concepts for this "new" competition and conflict space are hyper-connected and hyper-enabled SOF. These concepts use technology to ensure SOF has the situational awareness to outmaneuver its adversaries both physically and cognitively to achieve what the US Army calls "decision dominance."[1]

However, this policy paper argues SOF's desire for technology-driven, hyper-connected and hyper-enabled SOF is not a panacea. The technologies to enable these two concepts also emit signals and digital signatures which allow near-peer foes to detect and target SOF and disrupt or defeat special operations missions. Thus, like a double-edged sword, the same technology that SOF seeks to use in order to gain a competitive advantage over its near-peer adversaries is also potentially its Achilles' heel. This policy paper will offer six implications of hyper-connectivity and enablement and provide seven policy recommendations to minimize the risks to SOF of the above threats.

Background

The US military has spent two decades attempting to network the joint force and achieve decision dominance to "develop the situation out of contact, engage the enemy in unexpected ways, maneuver to positions of advantage with speed and agility, and engage enemy forces beyond the range of their weapons systems."[2] Today, the newest version of this concept in the US is known as joint all-domain command and control (JADC2).[3]

Likewise, SOF leaders envision a similar capability for SOF, placing technology as the key to dominance in the GPC to allow SOF operators and units to "see themselves; see the environment; and

The Kingston Consortium on International Security
138 Union Street, Suite 403
Queen's University,
Kingston, Ontario Canada K7L 3N6

kcis@queensu.ca

consortium partners

see the threat."[4] The goal is to allow SOF the ability to observe, orient, decide, and act faster than their adversaries.[5]

Central to the vision is the hyper-connected and hyper-enabled SOF operator with near-perfect, data-driven situational awareness and understanding as one part of the collective whole of similar operators, systems, and sensors. It envisions that the large-scale, interconnected sensor-operator combination will continually collect vast amounts of data from a variety of sensors, and rapidly analyze, compile, and turn the data into actionable intelligence helped by artificial intelligence and machine learning. In turn, SOF will use the finished intelligence to deliver multi-domain dilemmas against the adversary.[6]

The US Special Operations Command (USSOCOM) director of the hyper-enabled joint acquisition task force describes the technologies needed to achieve this vision including, "Edge computing and analytics…human-machine interfaces…adaptable and flexible sensors;…social network mapping… probabilistic techniques…that can speed and enhance decision-making; intuitive mobile applications that support data aggregation…and enhanced stand-off identification."[7] This compelling vision equips the practitioner with a panoply of capabilities at the forward edge of operations instead of at HQs and rear areas where such technologies are usually kept. As described, pushing these capabilities down to the "ground level" is attractive while the accompanying increased illumination of tactical elements expected to operate with a low signature is not.

USSOCOM's hyper-enabled operator is based on "four pillars of technology including communications, computing, data/sensors[,] and human-machine interfaces."[8] The goal is to ensure SOF operators or units are enabled with the information they need at the so-called "tactical edge."[9] Conceptually, it is difficult to argue against this hyper-connected and hyper-enabled SOF vision since it makes sense in a perfect world. However, the hyper-connected and hyper-enabled SOF concepts do not account for the reality of the threat environment and the capabilities of the near-peer adversaries to detect and target electromagnetic and digital signatures.

To work as advertised, the hyper-enabled operator must have secure, resilient, and sustained connections to the network and the bandwidths to send and receive substantial amounts of data. The scale of this hyper-connected network consisting of equally hyper-enabled operators and SOF units within a theater or globally is immense. The question is not if this hyper-connected network is secure—secure as in the data is secure from being decrypted—but whether it is detectable and targetable due to the immense electronic and digital signatures that such a network must emit.[10] In the zero-sum game of state competition, to expect or assume a large-scale, hyper-connected network consisting of hyper-enabled operators will not emit significant amounts of detectable and targetable signatures is unrealistic.

The points of greatest detectability and vulnerability are where the data intersects with the nodes—the nodes being the hyper-connected and enabled SOF operators and at SOF headquarters at all levels. The detection and then targeting of these nodes by near-peers, especially at scale and across multiple nodes simultaneously, will result in disruption or destruction of the hyper-connected and enabled SOF networks. Given the inherent risks of detection and targetability, it bears remembering that hyper-connectivity and enablement work both ways.

This risk does not go unacknowledged by SOF, but it tends to be assumed away. The USSOCOM Director of Science and Technology admits signatures are the norm in the future, "SOCOM will not be able to operate without an electronic signature….Going forward, operators will need to consider what type of

signatures they use and how long they can use it *without being detected* [authors' emphasis]."[11] However, how will the operators know if they have been detected, or will the gut-wrenching sound of an inbound precision missile, rocket, or artillery round on their position be the only indicator?

Given the lethality, precision, range, and ubiquity of modern weapons, the risk of underestimating this threat is high. Capabilities touted as "Low probability of intercept" expose the stark limitations of the technologies that SOF is expected to rely upon. Until there are "no-probability-of-detection" technologies, SOF will have significant exposure problems. This situation will get exponentially worse with the continued technological innovations to detect signatures and anomalies by near-peer powers.

Additionally, sensor technology abounds which will contribute to the exposure of SOF operators and operations. In the past, the various intelligence collection capabilities of near-peer adversaries were known and accounted for in mission planning. However, today, there are too many sensors to fully understand the threat. For example, publicly available data can expose SOF operators at home and abroad based on changes in their digital patterns of life.

This trend is especially disconcerting for clandestine SOF operators or operations as SOCOM's Science and Technology Director rightly notes, "An interconnected world also means less 'invisibility' for special operators who are accustomed to conducting clandestine missions." [12]

SOF must also be careful in employing what seems like sound solutions against unwanted detection and targeting. For example, US SOF's *naked operator* concept envisions deploying SOF "overseas with absolutely no electronic signature on them.… [procuring] local indigenous equipment[,] and then [blending] into the information environment, while still communicating back to their higher headquarters without raising a signature."[13] Although the recognition of the problem is the first step and should be applauded, the solution may be insufficient to protect operators operating in countries where our adversaries are hunting them but may fail to account for the realities of the big data world.

For example, entering a country with no signature is a signature. New signals from locally obtained equipment can be correlated with the arrival of foreigners whose actual identity and digital histories will be betrayed by big data. Smart city technology will quickly lead to the association of a "naked" operator and their devices via facial recognition. Data aggregation will make it difficult to obfuscate communication with higher headquarters. And lastly, if the adversary is tracking known or suspected SOF operators' digital patterns of life (POL) at home, they will be able to detect changes in their digital POLs when they are abroad.

Historical Vignettes

Modern SOF's forebearers, the World War II British Special Operations Executive (SOE) and American Office of Strategic Services (OSS) also experienced technology's benefits and risks. Long-range wireless communications were developed to support SOE and OSS efforts to organize, train, equip, and advise resistance elements and transmit critical human-intelligence reporting from occupied territories. This approach was a groundbreaking technological leap over traditional, non-technical clandestine communications means, such as couriers and carrier pigeons.

In response to the wireless, the Germans quickly developed a suite of counter-technologies—including fixed, vehicle, and later man-portable direction-finding capabilities that allowed the Germans to discretely find the exact building and floor of transmission and interdict the operator.[14] Despite efforts by SOE and OSS to adapt faster, the Germans relentlessly adapted

their counter-technology and operating procedures to effectively reduce the time needed to find and interdict transmissions.

Jump ahead six decades, and in 1997, an operation in Ansariya, Lebanon by the Israeli Defense Force's (IDF) maritime SOF unit, Flotilla 13, provides a catastrophic example of adversary exploitation of intercepted technology-emitted signatures. While executing a nighttime over-the-beach infiltration to conduct a raid, Flotilla 13 was ambushed by Lebanese Hezbollah, who killed 11 IDF SOF. Before the ambush, the IDF used cutting-edge drones to collect intelligence on the target. Underestimating Hezbollah's capabilities, the IDF repeatedly sent drones over the target not knowing that Hezbollah was able to intercept the unencrypted imagery transmission from the IDF drone and figured out the target of the raid.[15]

After the events of 9/11, the next decade saw a highly technology-driven SOF find, fix, finish, exploit, analyze, and disseminate (F3EAD) targeting process, fueled by insurgent and terrorist electronic and digital signatures. Throughout this period, SOF mastered the employment of counter-technologies at historic levels with agility and precision to relentlessly hunt the technology-emitted signatures of insurgent and terrorist leaders and their followers.[16] However, these low-tech adversaries quickly learned to deny their high-tech Western rivals a decisive victory by negating the West's technological advantage. Successful groups never allowed the Western coalition to decisively detect and engage their resilient clandestine insurgent and terrorist networks and threaten their overall ambiguity.[17]

While the coalition celebrated the death or capture of high-value targets, the clandestine networks simply replaced their losses, an accepted occupational hazard expected in their line of work, per their succession plans. This fact allowed these groups to protract conflicts and win by not losing in what they view as a multi-generational conflict where the goal is to not be decisively defeated or destroyed.[18]

Further examples abound. In a repeat of the signals compromise that led to the Flotilla 13 ambush, a similar compromise happened more than a decade later when Iranian-backed groups in Iraq reportedly used a $26 off-the-shelf software package to monitor US Predator drone feeds. In the fall of 2011, Lebanese Hezbollah reportedly correlated cellphone data to expose cellphone connections between US intelligence officers and their agents in Lebanon.[19] In 2018, reporting showed that US SOF among others had their operational bases compromised and patterns of life tracked by innocuous electronics, such as Fitbits, smart watches, and smartphone applications.[20] Also in 2018, it was reported that eight years earlier the Chinese government had begun to hunt and eliminate US-recruited agents in China by combining a tip from an espionage target with deep data analysis of aggregated historical data to detect and expose U.S. Government covert communications with their agents in China.[21] China's use of data, including stolen data, was further reported to have been the source of other exposures of US intelligence officers in Africa and Europe over the last decade as well.[22]

In 2020, cyber-sleuths or so-called "tail watchers" exposed the US SOF hostage rescue operation in Nigeria by identifying known US SOF aircraft departing the continental US and then staging and executing the rescue operations out of Europe.[23] Although they did not know the actual target, they quickly identified unusual activity and posted this information on social media, generating additional attention.

The continued clashes and short war between Azerbaijan and Armenia over Nagorno-Karabakh from 2020 to 2022 exposed the world to the realities of high-tech war, even for small states. One lesson

that should have been learned was the impact of technology, including signals emission detection, and the resultant exposure of forces on the modern battlefield. As Jack Watling noted, "Dependency upon radio in Western operations is a hard habit to kick….Western forces tend to leave a tell-tale map of electronic signatures….For a competent adversary [sic] these signatures offer another potent tool to map Western forces' movements."[24]

Cyber-sleuths are also exposing Russian nefarious activities and forces involved in the 2022 Russian invasion of Ukraine, both of which provide current examples that foretell the future for SOF in these environments. For example, the data analytics company Bellingcat successfully acquired data to piece together Russian activities, from identifying the team that poisoned Russian opposition figure Alexei Navalny to the exposure of Russian undercover operatives who spent years building and living their covers.[25] Additionally, in support of Ukraine's efforts to defeat the Russian invasion, hacktivists have used honeytraps, the allure of romantic encounters, to trick Russian troops into sharing their locations on social media sites, information later used for targeting.[26]

Lastly, like the way non-state actors used decentralization and mission command to remain resilient during the war against terrorism, the Ukrainian conventional and irregular ground forces are proving once again that asymmetries can be used to defeat more technologically capable foes. The Ukrainians are employing decentralized small units, using hit-and-run tactics and mission command, which can effectively attrit a technologically capable adversary. Stand-off weapons, whether remotely detonated improvised explosive devices or precision-guided munitions, increase the effectiveness and survivability of these small, decentralized forces by ensuring they do not become decisively engaged.

This sampling of historic vignettes begins to shed light on the threat of detectable signals or data of technology-emitted signatures, as well as potential means to counter more technologically capable adversaries. Although these vignettes do not show the impact of hyper-connectedness or hyper-enablement, they show the catastrophic results of even minor signal and data emissions and detection.

Risk of Technology Literature Review

Four recent articles raise similar alarms about the risks of signals and digital signatures and the use of other technologies, such as artificial intelligence (AI), in the GPC.

The first, Chris Cruden's 2021 "Manhunting the Manhunters: Digital Signature Management in the Age of Great Power Competition" highlights a general lack of understanding of the impacts of digital signatures by SOF and the need to "secure SOF operations now and in the future."[27]

The second article by Dr. Peter Roberts and Dr. Sandor Fabian, "More Odysseus, Less Achilles: Developing Special Operations Forces for the Challenges Ahead" addresses some of the inherent risks of focusing on technology instead of on SOF operators, which the authors surmise is likely to lead to nothing more than tactical success based on history.[28]

Third, is Dennis Murphy's "Sorting Through the Noise: The Evolving Nature of the Fog of War" which highlights the risks to the joint force (equally appliable to SOF) as it adopts AI to process mass data and AI's "inherent fallibility."[29] He also notes the need for military commanders and strategists to be comfortable with this reality and its implication.[30]

Lastly, Matthew Moellering's article focused on SOF and irregular warfare (IW), "Hiding in the Noise: Preparing the Irregular Warfare Community for the Age of AI," discusses similar issues with both

the positives and negatives of AI as applied by SOF and its adversaries and the need for SOF and IW practitioners to adapt to the realities and risks of big data.

These articles, published in the last 16 months are indicative of the increasing awareness of these issues and the need to heed these warnings. The services, led by the US Marine Corps (USMC), are also trying to understand and adapt to the threat of signature and data detection. Since 2016, the USMC has been preparing to fight in degraded or denied command, control, and communications environments.[31] Their clearly articulated goal is to "minimize signatures" in what they call the "battle of signatures" where "' to be detected is to be targeted is to be killed.'"[32]

Although not as far-reaching as the Marine Corps, the US Army has recently begun to understand the realities of the GPC and the threats of signals and digital technology-emitted signatures, addressing these risks in the recently released October 2022 Field Manual (FM) 3-0, *Operations*. It accounts for managing technology-emitted signatures as part of its acceptance of "constant enemy observation" and the resultant need to disperse and remain as mobile as possible. Finally, it stresses the need for leaders at all levels to be able to exercise "disciplined initiative cultivated through mission command," to over overcome uncertainty, dispersion of forces, and degraded communications.[33]

The Key Takeaways

The above highlights several trends and unintended outcomes related to overreliance on technology by SOF and the joint force as the means to gain an advantage over their adversaries. While theoretically the technology-driven concepts are well reasoned, technology continues to be a double-edged sword where the very same technology SOF looks to gain an advantage over an adversary can also be SOF's Achilles' heel. The adversary gets a vote and will not simply allow SOF and the joint force to gain an advantage without trying to counter it, negate it, or use it for their own advantage.

Based on the above, policymakers should consider the following six implications of SOF's efforts to achieve hyper-connectedness and hyper-enablement, including:

1. Providing near-peer adversaries the signals and digital signatures needed to detect, target, and achieve hyper-disruption or destruction of the SOF network;

2. Inadvertently tipping the balance from SOF being the hunter of the war on terrorism to SOF being the hunted in the great power competition or conflict;

3. Technology acquisition efforts resulting in greater, not lesser risk to SOF, and potentially higher SOF casualties when competition transitions to conflict against a near-peer adversary;

4. Challenging, at scale, the first SOF truth that people are more important than hardware where investment in and overreliance on technology overshadows efforts to recruit, assess, select, train, and retain the best SOF operators;

5. Raising the question of the viability of SOF's historical roles, missions, capabilities, and reliance on technology in the great power competition and conflict continuum; and

6. Demonstrating that more technology is not always the answer—dispersed and decentralized small units using mission command to mitigate and deny targetable signatures may be more practical in future near-peer fights.

Policy Recommendations

Based on the above implications, seven policy recommendations emerge if hyper-connected and hyper-enabled technology proves to be SOF's Achilles' heel:

1. Review hyper-connected and hyper-enabled SOF concepts and other technology-driven SOF concepts and capabilities to determine their applicability and risk to mission and risk to force in a great power competition or conflict.

2. Clearly define SOF's great power competition and conflict roles, missions, and the technologies required to identify and articulate the related risks to force and risk to mission.

3. Prepare SOF leaders and operators to be comfortable with operating without connectivity and tech-enabled situational awareness at the tactical, operational, and strategic levels, and to be able to seamlessly transition from digital to analog at the speed of war.

4. Take a page from the playbooks from clandestinely networked insurgent and terrorist adversaries and the Ukrainian conventional and irregular ground forces resisting the Russian invasion which have effectively avoided decisive action by disaggregating and dispersing their forces, used decentralizing command and control, to:

   a. Refocus on the first SOF truth—people are more important than hardware—and invest in SOF leader and operator training, education, and professional development to prepare and empower this and future generations of SOF to operate and thrive in a near-peer, high-threat, high-tempo, and disconnected environments of great power competitions and conflicts.[34]

   b. Fully accept mission command principles and practices which will require a complete cultural shift across the entire SOF chain of command from today's risk-averse and micromanagement culture.

   c. Exercise decentralized and dispersed operations using SOF maturity, expertise, competence, cultural awareness, and ability to operate in austere and denied areas.

5. Establish unbiased and continual red teaming to the SOF acquisition process and employment of SOF technology to assess the integrity, strength, and signatures of the technology throughout its life cycle.

6. Train SOF leaders and operators to understand and employ continuous signature assessments, management, and reduction at all levels to deny exploitable signatures to the adversary.

7. Consider similar policies for the joint force which will face similar risks but at a much large scale than SOF when developing and employing similar hyper-networked and hyper-enabled joint force concepts.

Conclusion

The goal of this policy paper was to challenge the traditional premise that technology is the answer to SOF's great power competition or conflict challenges. While the concepts challenged in this paper would be ideal in the perfect world, warfare is far from perfect or controllable, and thus the fog and friction of war, and near-peer adversaries with equal or greater technological abilities drastically increase the risk due to overconfidence in technological solutions.

Historically, while technology has offered many advantages to SOF and the joint force, adversaries have found its weaknesses, such as signal emissions, to turn the technology against its user. The technology-related risks increase with the threat's continued mastery of big data using artificial intelligence, machine learning, and quantum computing which

could correlate complex data streams even more rapidly in the future. Given these trends, it is difficult to see how SOF is going to hide in the digital and physical space without adapting current concepts to the realities of the threat environment.

This policy paper outlines six implications of SOF hyper-connectivity and enablement and seven policy recommendations to minimize the risks to SOF of the above threats. This paper, as well as the others mentioned above, should drive renewed interest in understanding the inherent risks related to hyper-connected and hyper-enabled SOF, and finding viable solutions to reduce the risks to SOF and SOF missions. If SOF finds its reliance on technology has surpassed its ability to operate without it to reduce signatures to a manageable level, then SOF will be relegated to non-near peer operations rather than against near-peers in great power competition and conflict.

Colonel (Retired) **Derek Jones** *is the Vice President of Valens Global and a retired U.S. Army Special Forces officer who served for 26 years in numerous special operations assignments including 10th Special Forces Group (Airborne), U.S. Special Operations Command Europe, U.S. Special Operations Command Central, and the interagency. He holds master's degrees from the U.S. Army War College, U.S. Army School of Advanced Military Studies, U.S Army Command and General Staff College, and the American Military University.*

Lieutenant Colonel (Retired) **Dan Leaf** *is a visiting Fellow of Vision Foresight, LLC, and served over 25 years as a U.S. Army Special Forces officer in command and staff positions in 20th, 7th, and 3rd Special Forces Groups (Airborne), the Joint Special Operations Command, an Army Special Mission Unit, and the interagency. He is a graduate of Virginia Tech.*

Endnotes

1 Headquarters, Department of the Army, ***FM 3-0 Operations***, (Washington, DC: Government Printing Office, 2022), https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36290-FM_3-0-000-WEB-2.pdf, accessed October 4, 2022, 3-13.

2 Donald Schenk, Daniel Bourgoine, and Brian Smith, "Unit of Action and Future Combat Systems – An Overview," ***Army AL&T Magazine***, January to February 2004, https://asc.army.mil/docs/pubs/alt/2004/1_JanFeb/articles/03_Unit_of_Action_and_FCS_200401.pdf, accessed August 10, 2022, 4-5.

3 Meredith Roatan, "Special Ops Software Office Takes on Pentagon Bureaucracy," ***National Defense Magazine***, May 2022, https://digital.nationaldefensemagazine.org/publication/?m=46185&i=745186&p=24&ver=html5, accessed August 8, 2022, 37.

4 Andrew White, "Special Forces Keep 'Eyes On' New Technology," ***ARMADA International***, May 8, 2020, https://www.armadainternational.com/2020/05/special-forces-keep-eyes-on-new-technology/, accessed August 8, 2022.

5 Ibid.

6 Stavros Atlamazoglou, "Why American Special Forces are on the Cutting Edge of Artificial Intelligence Technology," ***The National Interest***, December 25, 2021, https://nationalinterest.org/blog/reboot/why-american-special-forces-are-cutting-edge-artificial-intelligence-technology-198503, accessed August 8, 2022.

7 Yasmin Tadjdeh, "SOCOM Warrior: 'Hyper-Enabled Operator' Concept Inches Closer to Reality," ***Special Report: Special Operations Tech Review, National Defense Magazine***, 2020, https://www.nationaldefensemagazine.org/-/media/sites/magazine/ebook/specialops_ebook.ashx, accessed August 8, 2022, 18-19.

8 Ibid, 16.

9 Ibid.

10 Leonardo DRS, "Special Forces SATCOM for the Most Dangerous Missions in the World," ***SITREP: Review of DoD Technology Advancements***, Q2 2020, https://www.leonardodrs.com/sitrep/q2-2020-evolving-technology-keeping-sof-at-the-cutting-edge/special-forces-satcom-for-the-most-dangerous-missions-in-the-world/, accessed August 8, 2022.

11 Connie Lee, "The Quest for the 'Cyber-Secure' Hyper-Enabled Operators," ***Special Report: Special Operations Outlook, National Defense Magazine***, 2020, https://www.nationaldefensemagazine.org/-/media/sites/magazine/ebook/sofic_ebook_layout_2020.ashx, accessed August 8, 2022, 16.

12 Stew Magnuson, "Special Ops Tech Pulled in Different Directions," ***National Defense***, June 28, 2022, https://www.nationaldefensemagazine.org/articles/2022/6/28/special-ops-tech-pulled-in-different-directions, accessed August 8, 2022.

13 Kimberly Underwood, "Special Forces Command Seeks Key Data Aggregation, Cyber Tools," ***SIGNAL***, February 17, 2021, https://www.afcea.org/content/special-forces-command-seeks-key-data-aggregation-cyber-tools [Accessed September 11, 2022]

14 M.R.D. Foot, ***SOE: The Special Operations Executive 1940-46***, (University Publications of America, Inc., 1986), 107-108.

15 Yaakov Katz, "IDF encrypting drones after Hizballah accessed footage," ***The Jerusalem Post***, October 27, 2010, https://www.jpost.com/Israel/IDF-encrypting-drones-after-Hizbullah-accessed-footage, accessed October 5, 2022; and Siobhan Gorman, Yochi J. Dreazen, and August Cole, "Insurgents Hack U.S. Drones: $26 Software is Used to Breach Key Weapon In Iraq; Iranian Backing Suspected," The Wall Street Journal, December 17, 2009, https://www.wsj.com/articles/SB126102247889095011, accessed October 3, 2022.

16 Stanley McChrystal, ***My Share of the Task: A Memoir***, (New York: Penguin Group, 2013), 152-153.

17 Derek Jones, ***A Military Theory for Destroying Clandestine Insurgent and Terrorist Organizations***, (Carlisle Barracks, PA: United States Army War College, 2017), https://vdocuments.site/a-military-theory-for-destroying-clandestine-insurgent-and-terrorist-organizations.html?page=1, accessed October 3, 2022, 11-15.

18 Derek Jones, ***Understanding the Form, Function, and Logic of Clandestine Insurgent and Terrorist Networks: The First Step in Effective Counternetwork Operations.*** JSOU Report 12-3, (MacDill Air Force Base: The JSOU Press, 2012), https://apps.dtic.mil/sti/pdfs/ADA572767.pdf, accessed on September 17, 2022, 71-72.

19 Greg Miller, "Hezbollah damages CIA spy network in Lebanon," ***The Washington Post***, November 21, 2011, https://www.washingtonpost.com/world/national-security/hezbollah-damages-cia-spy-network-in-lebanon/2011/11/21/gIQA5uCEjN_story.html, accessed August 8, 2022.

20 Liz Sly, "U.S. soldiers are revealing sensitive and dangerous information by jogging," ***The Washington Post***, January 29, 2018, https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html, accessed August 8, 2022.

21 Zach Dorfman, "Botched CIA Communications System Helped Blow Cover of Chinese Agents," ***Foreign Policy***, August 15, 2018, https://foreignpolicy.com/2018/08/15/botched-cia-communications-system-helped-blow-cover-chinese-agents-intelligence/, accessed August 9, 2022.

22 Zach Dorfman, "China Used Stolen Data to Expose CIA Operatives in Africa and Europe," ***Foreign Policy***, December 21, 2020, https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks/, accessed August 9, 2022.

23 Chris Cruden, "Manhunting the Manhunters: Digital Signature Management in the Age Of Great Power Competition," ***Modern War Institute***, May 3, 2022, https://mwi.usma.edu/manhunting-the-manhunters-digital-signature-management-in-the-age-of-great-power-competition/, accessed August 8, 2022; Tom Demerly, "'SEAL Team Six' Makes Dramatic Predawn Hostage Rescue of American in Nigeria," ***The Aviationist Blog***, October 31, 2020, https://theaviationist.com/2020/10/31/seal-team-six-makes-dramatic-predawn-hostage-rescue-of-american-in-nigeria/, accessed August 8, 2022; and David Cenciotti, "Dissecting the U.S. Hostage Rescue Operations In Nigeria: Here Are All The Assets That Took Part In The Raid," ***The Aviationist Blog***, November 9, 2020, https://theaviationist.com/2020/11/09/dissecting-u-s-hostage-rescue-operation-in-nigeria-here-are-all-the-assets-that-took-part-in-the-raid/, accessed August 8, 2022.

24 Jack Watling, "The Key to Armenia's Tank Losses: The Sensors, Not the Shooters," RUSI, October 6, 2020, https://rusi.org/explore-our-research/publications/rusi-defence-systems/key-armenias-tank-losses-sensors-not-shooters, accessed November 2, 2022.

25 Aurelie Carabin, "How Bellingcat Became Russia's 'Biggest Nightmare,'" ***International Business Times***, September 7, 2022, https://www.ibtimes.com/how-bellingcat-became-russias-biggest-nightmare-3610435, accessed September 8, 2022; Bellingcat Investigation Team, "An Officer and a Diplomat: The Strange Case Of the GRU Spy With A Red Notice," ***Bellingcat.com***, February 25, 2020, https://www.bellingcat.com/news/2020/02/25/an-officer-and-a-diplomat-the-strange-case-of-the-gru-spy-with-a-red-notice/, access August 8, 2020; Bellingcat Investigation Team, "The Brazilian Candidate: The Studios Cover Identity of an Alleged Russian Spy," ***Bellingcat.com***, June 16, 2022, https://www.bellingcat.com/news/americas/2022/06/16/the-brazilian-candidate-the-studious-cover-identity-of-an-alleged-russian-spy/, accessed August 9, 2022; and Christo Grosev, "Socialite, Widow, Jeweller, Spy: How a GRU Agent Charmed Her Way Into NATO Circles in Italy," ***Bellingcat.com***, 25 August 2022, https://www.bellingcat.com/news/2022/08/25/socialite-widow-jeweller-spy-how-a-gru-agent-charmed-her-way-into-nato-circles-in-italy/, accessed August 26, 2022.

26 Giulia Carbonaro, "Hackers Honeytrap Russian Troops Into Sharing Location, Based Bombed: Report," ***Newsweek***, September 6, 2022, https://www.newsweek.com/hackers-honeytrap-russian-troops-sharing-location-base-bombed-report-1740070, accessed September 9, 2022.

27 Cruden, "Manhunting the Manhunters."

28 Peter Roberts and Sandor Fabian, More Odysseus, "Less Achilles: Developing Special Operations Forces for the Challenges Ahead," ***Modern War Institute***, West Point, January 13, 2022, https://mwi.usma.edu/more-odysseus-less-achilles-developing-special-operations-forces-for-the-challenges-ahead/, accessed August 8, 2022.

29 Dennis Murphy, Sorting Through the Noise: The Evolving Nature of the Fog of War," ***The Strategy Bridge***, September 10, 2022, https://thestrategybridge.org/the-bridge/2022/9/10/sorting-through-the-noise-the-evolving-nature-of-the-fog-of-war, accessed September 11, 2022.

30 Ibid.

31 Headquarters United States Marine Corps, ***The Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century***, Department of the Navy, September 2016, https://www.mcwl.marines.mil/Portals/34/Images/MarineCorpsOperatingConceptSept2016.pdf, accessed August 8, 2022, 6.

32 Ibid, 14; and Headquarters United States Marine Corps, ***Force Design 2030***, Department of the Navy, March 2020, https://www.hqmc.marines.mil/Portals/142/Docs/CMC38%20Force%20Design%202030%20Report%20Phase%20I%20and%20II.pdf?ver=2020-03-26-121328-460, accessed August 8, 2022, 13.

33 Headquarters, Department of the Army, ***FM 3-0 Operations***, (Washington, DC: Government Printing Office, 2022), https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36290-FM_3-0-000-WEB-2.pdf, accessed October 4, 2022, 3-2, 3-11, and 3-12.

34 United States Special Operations Command, SOF Truths, USSOCOM Webpage, https://www.socom.mil/about/sof-truths, accessed on November 3, 2022.