

# SPECIAL WARFARE

WRITING CONTEST WINNERS

COMBATING RUSSIA AND CHINA  
IN THE INFORMATION WAR

APRIL - JUNE 2021 | VOLUME 34 ISSUE 2



**STRATEGIC  
COMPETITION**

THE OFFICIAL PROFESSIONAL JOURNAL OF U.S. ARMY SPECIAL OPERATIONS FORCES

**ARTICLES**

07 | Order from Chaos in the Cognitive Space

14 | Influence at Echelon

22 | The Looming Threat of Synthetic Media

30 | Comprehensive Defense

**DEPARTMENTS**

FROM THE COMMANDANT \_\_\_\_\_ 04

MEMORIAL \_\_\_\_\_ 05

CAREER NOTES \_\_\_\_\_ 06

HUMAN PERFORMANCE \_\_\_\_\_ 33

BOOK REVIEW \_\_\_\_\_ 35

**ON THE COVER**

U.S. Army Photo Illustration



**SUBSCRIBE**

**OFFICIAL DISTRIBUTION TO UNITS:** Active Duty and Reserve special operations units can subscribe to *Special Warfare* at no cost. Just email the following information to [SpecialWarfare@socom.mil](mailto:SpecialWarfare@socom.mil)

- > Unit name / section
- > Unit address
- > Unit phone number
- > Quantity required

**INDIVIDUALS:** Personal subscriptions of *Special Warfare* may be purchased through the Government Printing office online at:

<https://bookstore.gpo.gov/products/sku/708-078-00000-0>

# SUBMISSIONS

**ARTICLE SUBMISSIONS:** *Special Warfare* welcomes submissions of scholarly, independent research from members of the armed forces, security policy-makers and -shapers, defense analysts, academic specialists and civilians from the U.S. and abroad.

Manuscripts should be 2,500 to 3,000 words in length. Include a cover letter. Submit a complete biography with author contact information (i.e., complete mailing address, telephone, fax, e-mail address).

Manuscripts should be submitted in plain text, double-spaced and in a digital file. End notes should accompany works in lieu of embedded footnotes. Please consult The Chicago Manual of Style, 15th Edition, for endnote style.

Articles that require security clearance should be cleared by the author's chain of command prior to submission. A memo of the security clearance should be forwarded with article. If the article talks about a specific theater special operations command, the article will be forwarded to the TSOC for clearance.

**PHOTO AND GRAPHIC SUBMISSIONS:** *Special Warfare* welcomes photo submissions featuring Civil Affairs, Psychological Operations and/or Special Forces Soldiers. Ensure that all photographs are reviewed and released by the unit public affairs officer prior to submission.

*Special Warfare* accepts only high-resolution (300 dpi or greater) digital photos; be sure to include a caption and photographer's credit. Do not send photos within PowerPoint slides or Word documents.

Photos, graphics, tables and charts that accompany articles should be submitted in separate files from the manuscript (no embedded graphics).

**SUBMISSION REVIEW AND PUBLICATION:** All submissions will be reviewed in a timely manner. Due to the volume of submissions we receive, we cannot reply to every submission. However, we do review and appreciate every submission. If your content meets the goals and requirements, we will be in touch. There is only one editor on staff and while in edit or layout phase of the upcoming magazine, new submissions will not be reviewed until complete.

Please note that submitted content is not guaranteed to be published in *Special Warfare*. There are several factors that determine what content is ultimately published including time and space availability, the approved editorial outline and theme, as well as relevance to the *Special Warfare* target audience and mission.

*Special Warfare* reserves the right to edit all contributions. *Special Warfare* will attempt to afford authors an opportunity to review the final edited version; requests for changes must be received by the given deadline.

No payment or honorarium is authorized for publication of articles or photographs. Material appearing in *Special Warfare* is considered to be in the public domain and is not protected by copyright unless it is accompanied by the author's copyright notice. Published works may be reprinted, except where copyrighted, provided credit is given to *Special Warfare* and the authors.

## FOR ADDITIONAL INFORMATION CONTACT THE SPECIAL WARFARE STAFF AT:

Commercial: (910) 432-5703

DSN: 239-5703

E-mail: [SpecialWarfare@socom.mil](mailto:SpecialWarfare@socom.mil)

## SUBMIT ARTICLES FOR CONSIDERATION TO:

E-mail: [SpecialWarfare@socom.mil](mailto:SpecialWarfare@socom.mil)

or via regular mail:  
USAJFKSWCS; Attn: AOJK-PAO;  
Editor, Special Warfare  
3004 Ardennes St, Stop A  
Fort Bragg, NC 28310

*Special Warfare* is an authorized, official quarterly publication of the United States Army John F. Kennedy Special Warfare Center and School, Fort Bragg, N.C. Its mission is to promote the professional development of special operations forces by providing a forum for the examination of established doctrine and new ideas.

Views expressed herein are those of the authors and do not necessarily reflect official Army position. This publication does

not supersede any information presented in other official Army publications.

Articles, photos, artwork and letters are invited and should be addressed to Editor, *Special Warfare*, USAJFKSWCS, 3004 Ardennes St., Stop A, Fort Bragg, NC 28310. Telephone: DSN 239-5703, commercial (910) 432-5703, fax 432-6950 or send e-mail to [SpecialWarfare@socom.mil](mailto:SpecialWarfare@socom.mil). *Special Warfare* reserves the right to edit all material.

Published works may be reprinted, except where copyrighted, provided credit is given to *Special Warfare* and the authors.

Official distribution is limited to active and reserve special operations units. Individuals desiring private subscriptions should forward their requests to: Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402. *Special Warfare* is also available on the Internet (<https://www.soc.mil/SWCS/SWmag/swmag.htm>).

# SPECIAL WARFARE

COMMANDING GENERAL & COMMANDANT  
MAJOR GENERAL PATRICK B. ROBERSON

EDITOR  
JANICE BURTON

ART DIRECTOR  
JENNIFER G. ANGELO



U.S. ARMY JOHN F. KENNEDY  
SPECIAL WARFARE CENTER AND SCHOOL  
*The Special Operations Center of Excellence*

**MISSION** The U.S. Army John F. Kennedy Special Warfare Center and School, The Special Operations Center of Excellence, assesses, selects, trains and educates disciplined Civil Affairs, Psychological Operations and Special Forces warriors and leaders, and develops doctrine and capabilities to support the full range of military operations — providing our nation with a highly educated, innovative and adaptive force.

**VISION** Forging experts in special warfare to adapt and succeed in a complex, multi-dimensional world through innovative training and education.

By Order of the Secretary of the Army

JAMES C. MCCONVILLE  
General, United States Army  
Chief of Staff

Official:

  
MARK F. AVERILL  
Acting Administrative Assistant  
to the Secretary of the Army  
2126708

# from the COMMANDANT



*Special Warfare* is the professional development publication for Army Special Operations. As such, our staff looks at what is happening in the world around us, and what is happening with our Army. That being said, it was not a great stretch for us to choose ARSOF's Role in Great Power Competition for the 2021 ARSOF Writing Competition.

Even as we fight wars against enemies on the field of battle, we are also waging a war of influence against familiar but evolving enemies: Russia and China.

In the Great Power Competition, we wage not only a war of information, but also continue to build alliances with our enduring partners and engage countries that, to date, have not had a seat at the table. In this environment every partner is important and what we bring and what they bring to the table is important.

The Great Power Competition leans heavily on our Civil Affairs and Psychological Operations regiments. The relationships these regiments have been building for years are becoming more and more important as we look at Special Operations Command Pacific and Special Operations Command South.

As you read this issue, you will see the efforts these regiments are putting forth, and coming as no surprise, the majority of these articles focus on their efforts around the world. We are in a war of words, a war of influence — and it is not one we can afford to lose.

A handwritten signature in black ink that reads "Patrick B. Roberson".

PATRICK B. ROBERSON  
MAJOR GENERAL, USA  
COMMANDING GENERAL

**“Though the object of being a Great Power is to be able to fight a Great War, the only way of remaining a Great Power is not to fight one.”**

— A.J.P. Taylor, historian



# NEVER FORGET

*A nation reveals itself not only by the men it produces  
but also by the men it honors, the men it remembers.*

*—John F. Kennedy*

**SFC WILL D. LINDSAY**

22 March 2019, Afghanistan  
*10th Special Forces Group (Airborne)*

**MSG MICHEAL B. RILEY**

25 June 2019, Afghanistan  
*10th Special Forces Group (Airborne)*

**SGM JAMES G. SARTOR**

13 July 2019, Afghanistan  
*10th Special Forces Group (Airborne)*

**MSG LUIS F. DELEON-FIGUEROA**

21 August 2019, Afghanistan  
*7th Special Forces Group (Airborne)*

**MSG JOSE J. GONZALEZ**

21 August 2019, Afghanistan  
*7th Special Forces Group*

**SFC DUSTIN B. ARD**

29 August 2019, Afghanistan  
*1st Special Forces Group (Airborne)*

**SFC JEREMY W. GRIFFIN**

16 September 2019, Afghanistan  
*1st Special Forces Group (Airborne)*

**SFC MICHAEL J. GOBLE**

23 December 2019, Afghanistan  
*7th Special Forces Group (Airborne)*

**SFC JAVIER J. GUTIERREZ JR.**

8 February 2020, Afghanistan  
*7th Special Forces Group (Airborne)*

**SFC ANTONIO R. RODRIGUEZ**

8 February 2020, Afghanistan  
*7th Special Forces Group (Airborne)*

## ANNOUNCEMENTS

### 1st Quarter FY22 Army Boards

03 OCT 2021	MG, Army PSB
04 OCT 2021	BG AMEDD PSB
05-22 OCT 2021	LTC ARMY (OPS, OS, FS, ID) PSBs and MAJ SELCON
05 OCT 2021	FY22 TRADOC 2ND Command Board
06-22 OCT 2021	COL ARMY (OPS, OS, FS, ID) PSBs
18-22 OCT 2021	FY23 LTC AMEDD CSL Board
19 OCT - 2 NOV 2021	RA-USAR AGR SFC Evaluation Board
25 OCT 21	FY22 ARNG GO Federal Recognition
26-29 OCT 2021	FY22 USAR GOAAB & FY21 USAR GOVPB
07-10 NOV 2021	BG ARMY PSB
08-24 NOV 2021	RC COL APL PSB and LTC APL SELCON
16-19 NOV 2021	COL MC / DC PSBs
16-19 NOV 2021	RC CO L & LTC CH PSB and MAJ CH SELCON

### Army Career Intermission Program

Army published Army Directive 2021-15, Army Career Intermission Program, on 6 MAY 2021. This permanent retention authority applies to Regular Army (RA) and U.S. Army Reserve (USAR) Active Guard Reserve (AGR) Soldiers.

This is a one-time temporary transition from active duty RA or USAR AGR to Individual Ready Reserve (IRR) to allow Soldiers to meet personal or professional needs while providing a mechanism to return to active duty. The long-term intent of CIP is to retain the valuable investment in experience and training the Army would otherwise lose when Soldiers separate permanently. Under CIP, Soldiers will retain certain benefits and return to active duty (RA to RA, AGR to AGR) at the end of the inactive duty period.

The period spent in the CIP may not exceed three years. The AD addresses eligibility, pays, active duty service obligation and adjusted service computation upon the Soldier's return.

## SPECIAL FORCES

### Direct Commission to CW2

On May 12, 2021, as part of the Army Talent Management Task Force's innovative measures to modernize officer career management, the acting Secretary of the Army signed the Army Directive 2021-19, Direct Appointment of Senior Non-Commissioned Officers to the Grade of Chief Warrant Officer 2 in Special Forces. This policy, part of a two-year pilot, gives SF the ability to tailor specific accession criteria based on modernization requirements and allows direct commission for specific senior NCOs to CW2 following the 18-week Special Forces Warrant Officer Technical and Tactical Certification Course. The Direct Commission to CW2 initiative is designed to attract the most qualified CMF 18 NCOs to serve as assistant detachment commanders or detachment commanders on an Operational Detachment -Alpha. SF Branch set parameters for DC to CW2 based on individual experience, training and education. Eligibility criteria for DC (in addition to all prerequisites required by SF and HQDA/USAREC) are:

- (1) Serving as a Sergeant First Class (E-7) with minimum of one-year time in grade at time of application or above.
- (2) Have a minimum of 60 months experience at the SFOD-A/E/G level.
- (3) Minimum of an associate degree or 60 college credit hours from an accredited university.
- (4) Emerald Nomad qualified.
- (5) Must maintain a 90 percent or above grade point average, meet height/weight standards and pass all physical assessments (without retesting a physical event) during SFWOTTC. DC candidates unable to conduct physical assessments due to injuries sustained during SFWOTTC will be assessed on a case-by-case basis.

Applicants meeting the prerequisites for DC to CW2 must obtain endorsement through the Group Commander's Letter of Recommendation and approval from the USAJFKSWCS Commanding General. Direct Commission of a NCO to CW2 acknowledges the diverse and unique requirements of SF. This directive allows SF to address critical manpower gaps with exceptionally qualified people to enhance readiness for the SF Regiment.

## EDUCATION OPPORTUNITIES

### Naval Postgraduate School

Naval Postgraduate School is an 18-month MEL-4 and JPME-1 producing program open to eligible 18A, 37A and 38A officers. Eligible officers are those considered by the FY21 Major, Operations, Operations Support, Force Sustainment and Information Dominance Promotion Selection Board. MILPER 21-018 identifies the Promotion Selection Board Zones of Consideration. MILPER 21-48 and its amendment 21-148 provide application details. All NPS coursework occurs at Monterey, CA.

- There are three curriculums available to applicants:
- 697 – Applied Design for Innovation (18A & 38A)
  - 698 – Joint Information Strategy and Political Warfare (37A)
  - 699 – Special Operations and Irregular Warfare (18A & 38A)

### National Defense University

Joint Special Operations Master of Arts program awards credit for the Advanced Operations Course for Officer applicants. Officers are still required to complete the Intermediate Level Education Common Core Course separately to achieve MEL-4. The JSOMA is a fully accredited 10-month Master of Arts in Strategic Security Studies at Fort Bragg, N.C. This program is the same as the NDU's College of International Security Affairs. This program is open to eligible Officer, Warrant Officer and Non-commissioned officer applicants. A MILPER message identifying eligibility criteria is pending publication, when available this information will also go out USASOC-all.

APPLICATION REQUIREMENTS	NPS	NDU
Updated Record Brief- no photo	X	X
Last 3 year's evaluation reports – must reflect 3 years	X	X
DA Form 1618 – endorsed by first O-6 in Chain of Command	X	X
HRC Branch Approval Memo signed by Career Manager	X	X
Statement of Purpose – Academic Essay Format min 250 words/max 1000 words detailing research interest and how it will support Special Operations	X	X
NPS Conditional Acceptance Letter	X	
Signed Research Agreement	X	X
Signed and initialed Student Acknowledgement of Responsibilities		X
Official Undergraduate Transcripts	X	X



# ORDER FROM CHAOS IN THE COGNITIVE SPACE

## Civil Affairs in the Great Power Competition.

BY COLONEL JOHN WILCOX, LIEUTENANT COLONEL SAMUEL HAYES AND MAJOR ASSAD RAZA

**"To win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill."**

— Sun Tzu, *The Art of War*<sup>01</sup>

In the information age, misinformation campaigns and new technological tools are pivotal in gaining an edge over competitors across elements of national power: diplomatic, information, military and economics. Competitors such as Russia and China employ a calculated mixture of information with other power instruments to advance their interests below the armed-conflict threshold.<sup>02</sup> To be successful, Army Special Operations Forces must maximize Civil Affairs capabilities to understand the breadth of a competitor's strategic intentions and capabilities to gain a competitive advantage against peer nations.

The 2018 National Defense Strategy states that the United States must restore its competitive military advantage to deter Russia and China.<sup>03</sup>

Regaining that advantage must go further than any one aspect of national power and requires an integrated policy with additional permissions and authorities. According to the NDS, "America is a target, whether from terrorists seeking to attack our citizens; malicious Cyber activity against personal, commercial or government infrastructure; or political and information subversion."<sup>04</sup> For these reasons, U.S. Forces must anticipate and exploit the information environment to deter aggression in the homeland.

Joint Doctrine Note (JDN) 1-19, *Competition Continuum*, provides the joint force a base outline of power competition. JDN 1-19 includes a description of competition below armed conflict as:

Competition below armed conflict tends to occur over extended

periods of time. In comparison to armed conflict, actions are often more indirect and the expenditure of resources less intense, thus allowing for a more protracted effort. As an inherently constrained and measured approach, it is not generally used by competitors requiring quick results. For the joint force to successfully campaign through competition below armed conflict, it should adopt a similar long-term approach but one supple enough to react to rapid changes in the political, diplomatic and strategic environment.<sup>05</sup>

As recommended in the JDN 1-19 description, the joint force should adopt a similar approach to our competitors. This approach includes information campaigns to exploit partisan disputes based on abuses towards marginalized groups, such as human rights violations against minority sects of a population. The United States can also exacerbate local divisions between

PHOTO ABOVE

A group of protesters gather following the death of African-American George Floyd. From democratic elections to racial tensions, America's issues polarize its population and are dangerous vulnerabilities, translating into physical flashpoints providing nation-state competitors an opportunity to weave flashpoints together and erode trust within the U.S. borders and abroad. U.S. ARMY PHOTO BY SPC. JOVI PREVOT

competitors and their people, as do the U.S. peer competitors.

Russia and China weaponize information using the 4D (Dismiss, Distort, Distract and Dismay) framework to achieve strategic advantages in the information and physical spaces to develop an alternative narrative to an event.<sup>06</sup> The DFR Lab described the 4D framework as the ability to dismiss the critic, distort the facts, distract from the main issue and dismay the audience.<sup>07</sup> Although DFR Lab's studies primarily focused on Russia, this framework can be used by any adversary, state or non-state actor, to create an alternative narrative to the truth. In a time of enduring competition in the cognitive and information space, winning the narrative will be critical for the United States throughout the competition continuum.

U.S. competitors use the 4Ds to incite uprisings and divide societies. In the book *Like War: The Weaponization of Social Media*, the authors added a fifth "D," which stands for "division."<sup>08</sup> The added fifth "D" includes describing adversaries' intent to provoke targeted populations to increase divisions between them and their governments. The authors provided insights on

how adversaries use social media to influence actions on the ground, from inciting protests to election outcomes.

Even though Russia and China continue to dominate in the competitive space, the U.S. remains behind in implementing a strategy using an offensive 4D approach. This uneven approach contributes to competitors' exploitation of current U.S. tensions, creating domestic issues that negatively impact the country. These realities negatively impact all elements of national power to include the military. Therefore, preparing to conduct offensive and defensive operations become more critical as competitors evolve and the environment increases in complexity.

### TOOLS TO EXPLOIT THE COMPETITIVE SPACE

The use of the cognitive and information space to influence populations is nothing new. American psychological operations and information campaigns trace their lineage back earlier than the Spanish American War. Information and cognitive battlefields receive fewer

resources and attention compared to the conventional fight. Efforts to incorporate Information Operations, Civil Affairs, and Psychological Operations into Combat Training Center events illustrate progress; however, the evaluation for unit commanders does not include their ability to wield influence over an enemy force, nor are they reprimanded if they fail to understand the populations where the fighting occurs.

In the U.S. military, information-related capabilities are the tools available for employment underneath the IO umbrella. IRCs in the military usually include military information support operations, also known as PSYOP, military deception, operations security, public affairs, electronic warfare, civil affairs operations and cyberspace operations. The synchronization of these tools allows the joint force commanders to affect target audiences throughout the three dimensions of the information environment: physical, informational, and cognitive, as seen in *Figure 01*. As this figure demonstrates, achieving effects in the information environment takes a greater understanding of the factors in the three interrelated dimensions. Strategists must use these tools in conjunction with appropriately scoped military capabilities and incorporate them across multiple means of competition. For ARSOF, Civil Affairs and PSYOP possess innate information and influence skills and the ability to leverage human networks. Civil Affairs forces aid with understanding the information environment.

CA forces as an IRC contribute to information campaigns by gathering critical information on the physical and cognitive dimensions, as seen in *Figure 02*. CA collects this information through civil reconnaissance and civil engagement activities. For example, CA can identify communication infrastructure for potential use through civil reconnaissance and validate population demographics in a dynamic environment. Additionally, by engaging with local populations, CA can assess whether messages resonate with local communities and critical mobilizers to assist PSYOP with their target audience analysis.

**FIGURE 01: INFORMATION ENVIRONMENT DIMENSIONS**

Types	Affects	Examples
Physical	Content	<ul style="list-style-type: none"> <li>The physical world and its content, particularly that which enables and supports exchanging ideas, information and messages.</li> <li>Information systems and physical networks.</li> <li>Communications systems and networks.</li> <li>People and human networks.</li> <li>Personal devices, handheld devices and social media graphical user interfaces.</li> <li>Mobile phones, personal digital assistants and social media graphical user interfaces.</li> </ul>
Informational	Code	<ul style="list-style-type: none"> <li>Collected, coded, processed, stored, disseminated, displayed and protected information.</li> <li>Information metadata, flow and quality.</li> <li>Social media application software, information exchange and search engine optimization.</li> <li>The code itself.</li> <li>Any automated decision making.</li> </ul>
Cognitive	Context	<ul style="list-style-type: none"> <li>The impact of information on the human will.</li> <li>The contextualized information and human decision making.</li> <li>Intangibles, such as morales, values, worldviews, situational awareness, perceptions and public opinions.</li> <li>Mental calculations in response to stimuli, such as liking something on a social media application.</li> </ul>



Ultimately, as a sensor on the ground, CA can visualize and influence relationships, depicting the common civilian operating picture for IRCs to synchronize and shape the competitive environment in a manner aligned with the U.S. goals and objectives.

Aggregated and synthesized information aids in a clearer picture of what is unknown in competition, as seen in *Figure 03*. CA provides civil information and, when analyzed with threat information from the S-2, contributes to situational awareness, lethal and non-lethal targeting and shaping operations. Improved awareness across the operational variables enables a leader to better compete by observing adversaries quicker, influencing opponents' vulnerabilities directly and indirectly and competing at a time and place of the leader's choosing. This awareness enhances the unity of effort across a whole-of-government approach to pool and preserve combat power below the threshold of conflict.

Combining these capabilities helps compete across all three dimensions and use these spaces to develop and execute coordinated activities to influence behaviors or actions at a target audience. Such efforts enable the convergence of discrete skills specifically designed to address competition outside of a purely conventional approach. For the U.S. Army, these capabilities primarily reside in SOF and can counter adversaries seeking to compete in these unique spaces.

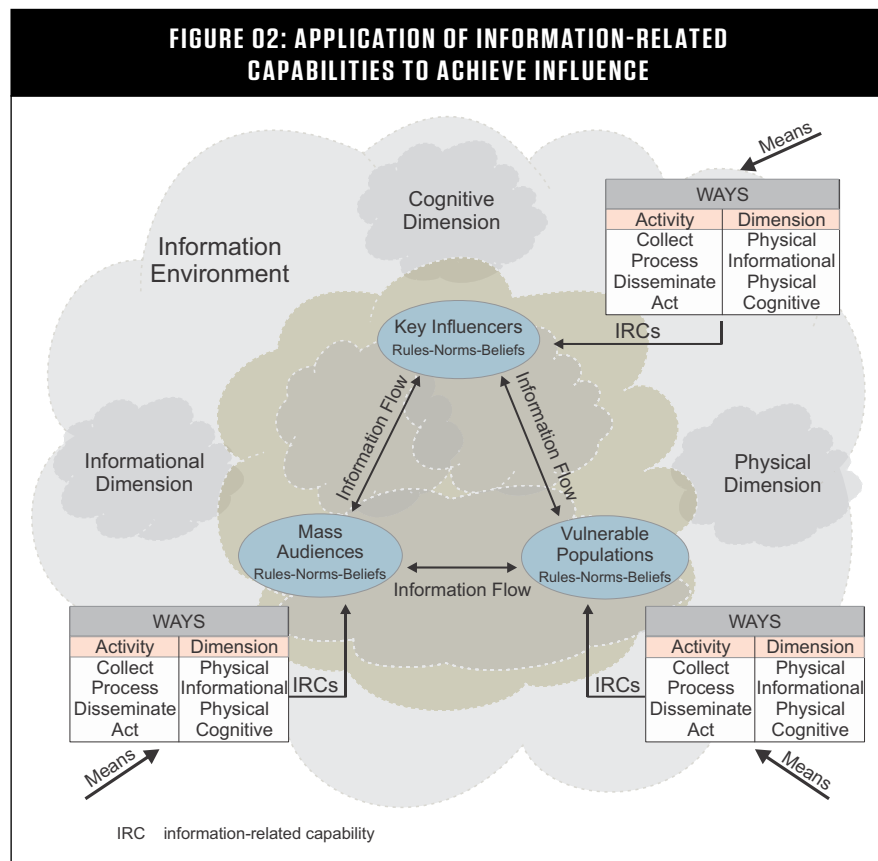


Figure 02 From Joint Publication 3-13, *Information Operations*

### CASE STUDY: SPACES FOR FOREIGN NATIONS TO COMPETE

The U.S. information space is sophisticated and contested. In 2016, Russia demonstrated to the world that they could interfere in U.S. elections.<sup>09</sup> In 2020, the tragic death of African American George Floyd at the hands of white police opened deep racial wounds that pushed Americans further apart

amid the COVID-19 pandemic.<sup>10</sup> From democratic elections to racial tensions, America's issues polarize its population and are dangerous vulnerabilities, translating into physical flashpoints. Domestic vulnerabilities provide nation-state competitors an opportunity to weave flashpoints together, resulting in eroded trust within the U.S. borders and abroad, creating a tipping point on the international stage — demonstrating failed leadership.

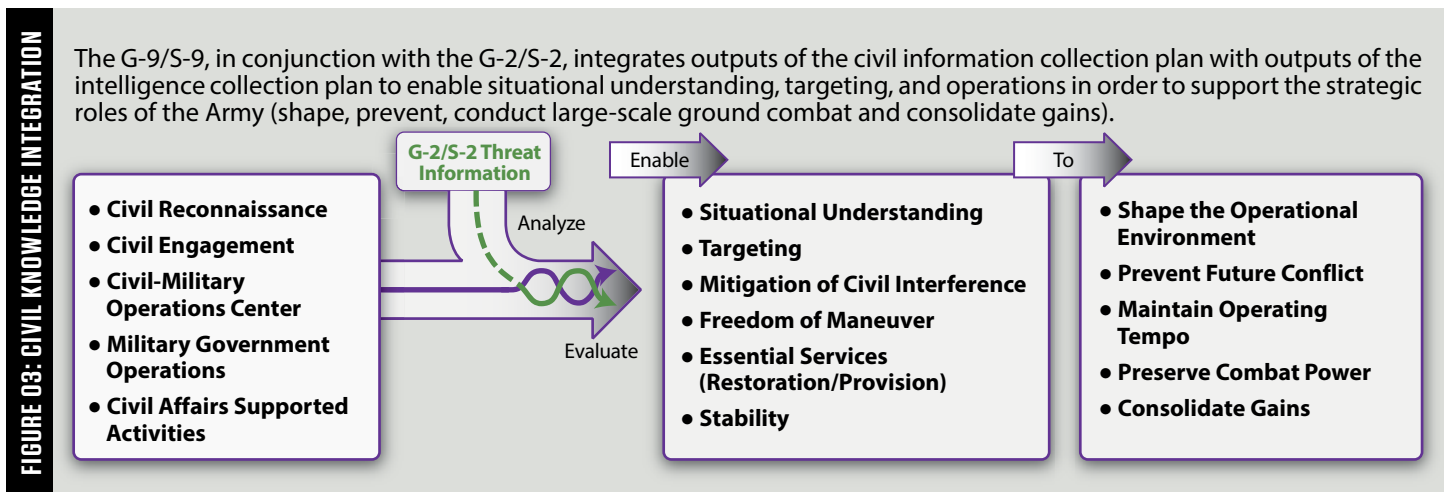


Figure 03 From Field Manual 3-57, *Civil Affairs Operations*

Navigating the nuanced layers of PMESII (Political, Military, Economic, Social, Information, and Infrastructure) can be a challenge in this environment, highlighting the importance of coordinated response. In response to Minneapolis, Minnesota, people, groups, and organizations worldwide took to the Internet to voice their opinions about George Floyd’s death. These groups, which included those in opposition to America’s ideals, intertwined among Americans exercising their constitutional right to protest. The information in the cognitive space tends to “echo” as ideas are shared among like-minded individuals. The algorithms that drive social media systems tend to group into like-minded silos, where the more outrageous claims and assertions get more clicks, likes and view time.<sup>11</sup> As the racial divide widens, the echo chambers grow across mainstream media, and the silos deepen in ideological camps, the cumulative effect entrenches opposing viewpoints and reduces a unified national response to the crisis. The resultant fog in the information space creates fertile ground for state actors, like Russia or China, seeking to exacerbate ideological fissure points domestically.

Unpacking this conflict space around Portland, Oregon, helps to understand what could occur by adversaries in the United States. In July 2020, senior Department of Homeland Security officials portrayed Portland as a city under siege.<sup>12</sup> With the chaotic events unfolding, one could observe many actors — Portland Police, U.S. federal agents, Black Lives Matter activists, protesters, Antifa and armed militia groups. These actors are but a few among those fighting for control in individual physical spaces and attempting to advance specific interests and win the narrative within the United States and abroad. *Figure 04* includes a map of the diverse group of actors vying to voice their grievances, some wanting the status quo and others desiring change. Such complexity highlights the difficulty U.S. military leaders will face in competition.

Understanding the complexity of the competition environment is difficult, even for a seasoned military leader. *Figure 04* illustrates such a competitive space and is a graphical depiction of the groups and individuals who influence that competition

environment. A military leader’s challenge is to identify potential opponents and supporters in this dynamic environment and determine windows of opportunity to gain the advantage. As more outside groups inundate the area and opportunists or state actors who foment unrest makes understanding this environment a challenge. Analysis of civil factors (i.e., ethnic groups and household income) highlights vulnerabilities like racial tensions and economic disparities.<sup>13</sup> In 2012, a study identified that the Portland downtown area was critically vulnerable across race, economics, and educational factors. After George Floyd’s death, these elements became a flashpoint, transforming into a hotly contested issue whose proponents fell into political camps in the United States and abroad.

Military leaders need to understand how to maneuver within this information space and how it connects to the physical space. To further develop this idea, Portland, Oregon, is an example of how a military leader might link the physical space and the information space. Threats of violence and violent rhetoric enabled the most

**FIGURE 04: PROTESTS IN PORTLAND OREGON – BEYOND 170 DAYS**  
*Goerge Floyd died on May 25, 2020, protesting started on May 28,2020*

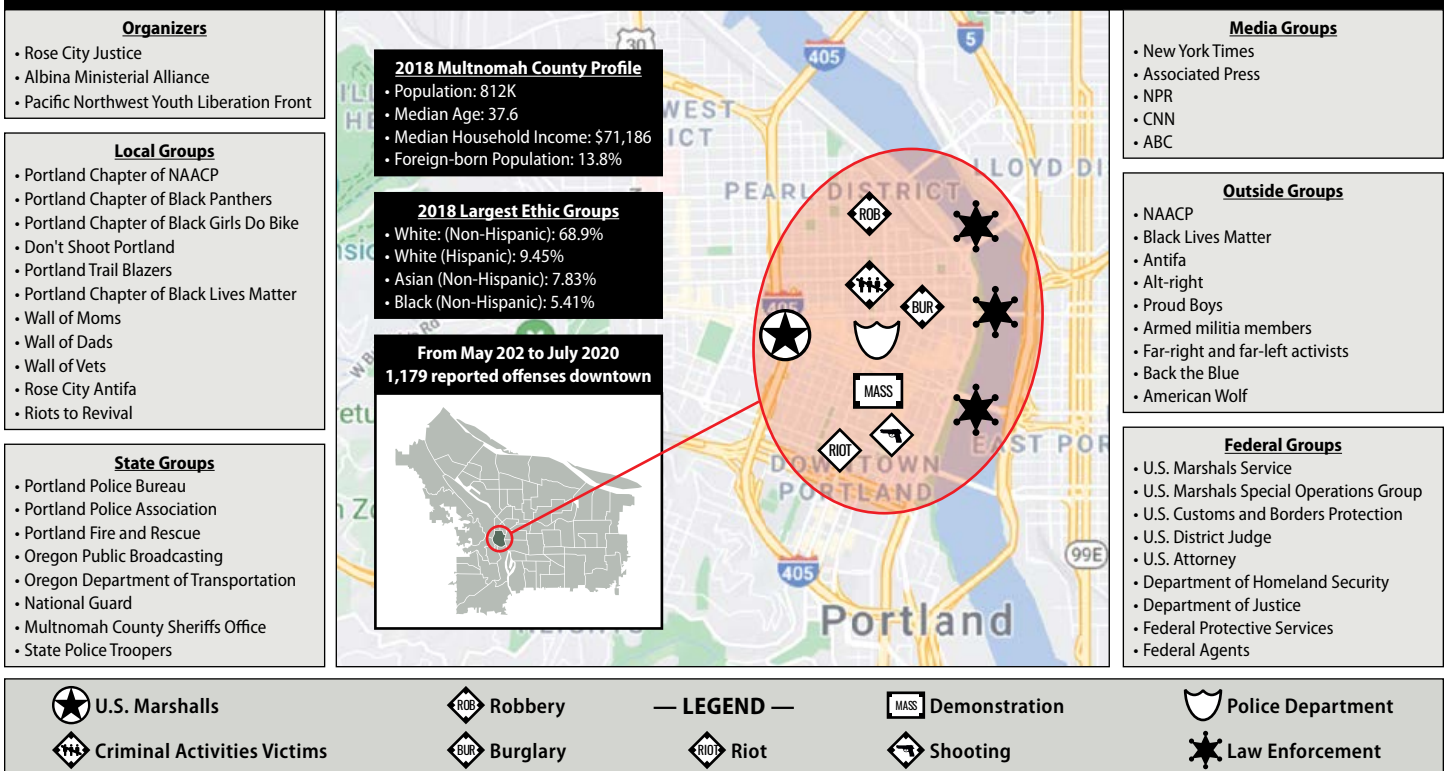
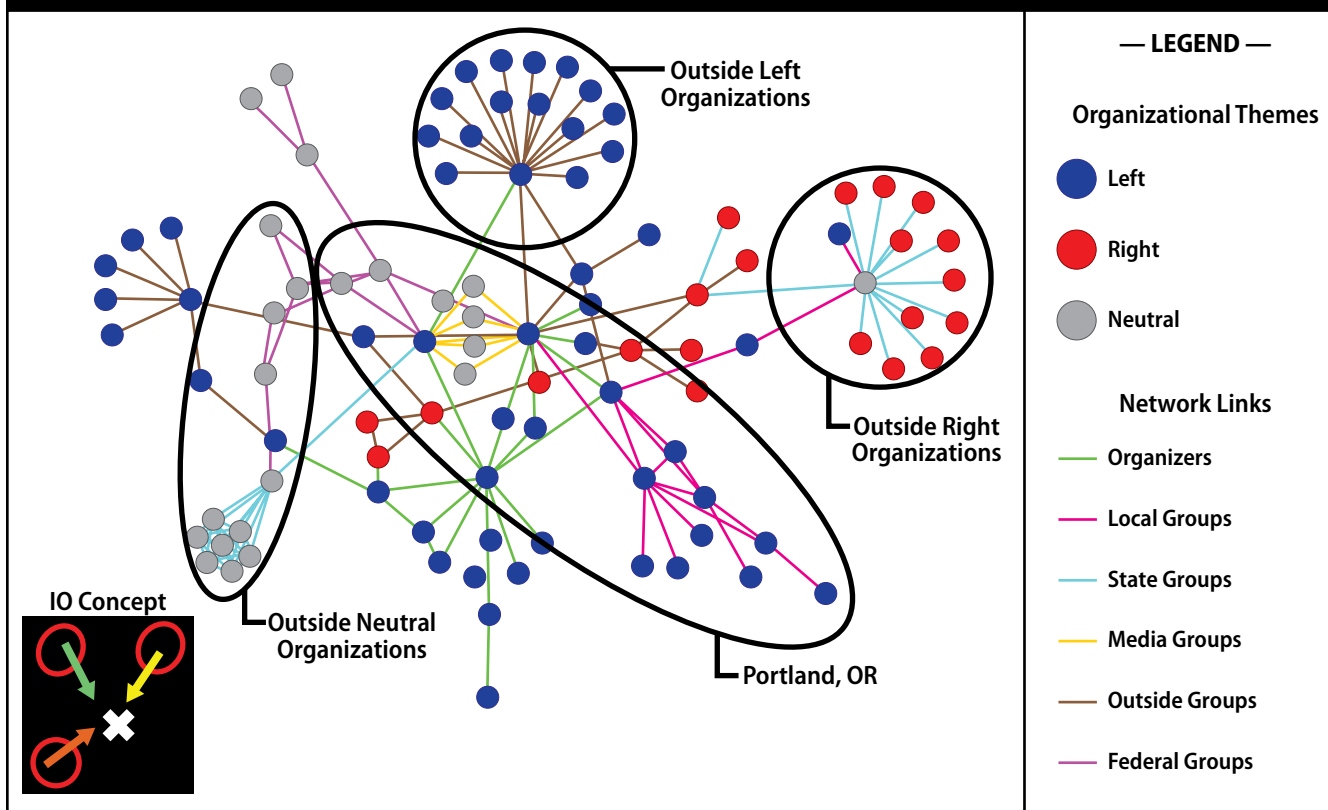


FIGURE 05: THE COMBINED PORTLAND NETWORK



motivated and radicalized to connect and support one another. This support ultimately manifested in multiple riots and property damage, while a concurrent information campaign condoned the actions. Legitimate protests and violence were lumped together, which further fomented anger and political division in the information space and complicated the law enforcement response. This dilemma underscores the importance of information campaigns as complementary operations, assisting with securing the objective.

In Portland, an opposing force with CA-like capabilities has multiple options to exploit the competitive space. Russia and China operate below the threshold of war because they can reach their goals in this emerging unconventional space. For instance, in the early competition phase of operations, CA would enable disinformation by mapping the human network, finding the crucial players or organizations within that area aligned to particular interests and mobilize to converge at will. Interacting with this network, whether friendly, neutral or a threat, must be done simultaneously from the tactical to the strategic levels,<sup>14</sup>

which illuminates the best option to engage the network by strengthening or weakening identified relationships to reach the goal of discord.

Specifically, soldiers with these CA-like capabilities can determine who or what is influential in the network through the analytical technique of human network analysis, allowing commanders three ways to engage the network (i.e., support, influence and neutralize) across the range of military options.<sup>15</sup> Supporting the various networks means to assist the individuals, groups, organizations in the network, or for members within the network to perceive they have gained assistance towards their ideals, causes and goals.<sup>16</sup> Influencing the network's purpose is to shift attitudes, perceptions and behaviors of key network elements to aid with the commander's objectives.<sup>17</sup> When the former two activities fail, one can attempt to neutralize the network, rendering the enemy incapable of interfering or reaching their goals. HNA works with six methodologies to accomplish network engagement; social network analysis aided in understanding Portland.

Social network analysis, not to be confused with link analysis or social

media, is a collection of theories and methods that explores the patterns of ties (relations) among and between actors.<sup>19</sup> While the actors in networks are often individuals, they can also be groups, corporations, nations, etc.<sup>20</sup> The most common metrics for identifying key actors are centrality measures, which are more than 40 centrality measures, all of which have different assumptions of what makes an actor central. A central actor can be an actor who has numerous ties to other actors, like a class president (degree); is closer to all other actors, like someone who resides in many friend groups (closeness); lies between different pairs of actors, like a bridge between jocks and academics (betweenness); or has ties to other highly central actors, like a godfather (eigenvector).<sup>21</sup> In some networks, the same actors score high on all four measures. In others, they do not. However, these measures help understand the relationship between actors, but it also helps with visualizations. *Figure 05* illustrates the Combined Portland Network conducted via open-source (i.e., Internet, magazines, articles, etc.) from May 25 to August 25, 2020.

The Combined Portland Network provides a better picture at the organizational level of analysis for the

adversary to plan and act. SNA aided with exploring the relationships among groups connected to the map results in more than 100 organizations identified in the above visualization. The authors used the following legend to interpret the network: each organization is represented by a node, and colored by political affiliation. A colored link between the nodes represents each of the six CPN networks. These lenses aid a commander in going more in-depth into Portland and getting a sense of stakeholders' complexity and influences. Therefore, the beginnings of physical, informational and cognitive space unfold. The black circles indicate different groupings of organizations from those who operated in Portland, physically, to those outside organizations that could

05 provides an information concept to reach adversarial goals in Portland, Oregon; their plan could be to flood the zone with outside actors inflaming the local situation and turn it into a political issue, showing a high degree of distrust. An adversary could create physical violence with the intent of generating additional political polarization through politically aligned organizations' while simultaneously eroding faith in the government.

Furthermore, an adversary could use teams' mixture of capabilities across CA, PSYOP, SF, IO and the intelligence spectrum, on the ground as instigators. In this case, adversarial units would leverage proxy forces while providing distance and deniability. In the informational space, units analyze divisive sentiments

within this space. With this competition being unconventional, ARSOF has the right tools to innovate and lead as the force of choice for the United States to compete against Russia's and China's decisive advantage as they create their strategies for the next century.

## CONCLUSION

The Army's focus on great power competition is exactly the right one. However, military strategists continue to focus on the wrong kind of battlefield. The global and emerging powers at odds with the United States learned the lessons of 21st-century warfare; focusing on conventional warfare means the competition occurring elsewhere goes unresolved. Nations now fight wars in the

# THE GLOBAL AND EMERGING POWERS AT ODDS WITH THE UNITED STATES LEARNED THE LESSONS OF 21ST-CENTURY WARFARE ... NATIONS NOW FIGHT WARS IN THE INFORMATION, COGNITIVE, AND ECONOMIC SPACES WHERE THE LOSSES ARE BLOODLESS BUT NO LESS DEVASTATING AND IMPACTFUL.

influence the area. Politically left-aligned organizations reinforce outside the area to assist with resources and support; politically aligned right organizations enter the space to counter the left's message. The right-aligned organizations also have an extended network beyond Portland. The neutral organizations represent the government, local authorities, media and research institutions. As the situation worsens, additional organizations join the space. As this competition space unfolds, the media captures their understanding of the ground truth for all to analyze.

An adversarial information campaign spreads disinformation and discord through the network. *Figure 05* implies that civil vulnerabilities located in the United States could be exacerbated from anywhere, providing the opponent standoff and anonymity. The racial and economic undertones embedded in Portland create an ideal environment for exactly such an opponent. The bottom left of *Figure*

and spread these false statements across the information space; in the cognitive space, units would distribute disinformation to legitimate outlets to gain traction over American airwaves. If successful, this campaign offers a series of follow-on operations with the potential for severe impacts on the economy, the information space and the government. Such a combined campaign would strengthen the narrative of failing leadership.

As military leaders reflect, the following questions help one consider the U.S. role within great power competition. Reflecting on the above scenario or real-world events, one has to ask, was the network influenced? Did the perceptions, attitudes and behaviors change? If so, why? These questions represent the realities of today's military leaders. However, as an Army and leaders, capabilities like Civil Affairs exist to understand the human networks within the civil component, and more emphasis needs to be on training formations to compete and maneuver


information, cognitive, and economic spaces where the losses are bloodless but no less devastating and impactful.

As stated in China's overarching plan to become a world leader, today's windows of opportunity provide China time and space to seize the initiative and move closer to their goal.<sup>22</sup> Russia can also gain the advantage by reducing or removing American influence worldwide, enabling the ability to reshape the international order. As illustrated in September 2020, the events depict an increase in skirmishes on fringes of the network between the left and right politically aligned organizations beyond Portland, expanding through the United States.<sup>23</sup> Such conflicts have some scholars asking questions such as: is America in the early stages of armed insurgency?<sup>24</sup> Questions like these cause the United States to reflect as China and Russia move into its periphery. Some might argue that other nations contributed to the worsening of the situation; other people would say the opposite.



Either way, one must admit something happening. Therefore, as indicated in this narrative, CA provides critical capabilities that can help leaders today and, in the future, understand and influence the environment they will shape, fight, and win to ensure American leadership remains steadfast.

As this paper lays out, the United States and our competitors already possess the means to fight in the competition space. However, outmoded views on warfare that focus strictly on a conventional fight impede the development and advancement of policies, strategies, weapons, and training to meet the fight. It is time for the U.S. Military to focus on the competition space away from a conventional battlefield and ensure the military is prepared to engage with other large scale nations. This approach balances action across the spectrum of

competition and ensures our competitors cannot exploit those gaps where the United States military is not fully prepared to fight in these ongoing and very real conflicts. 

## ABOUT THE AUTHORS

**COL John Wilcox** is an active-duty Civil Affairs officer and current student at the United States Army War College. He has 15 years of experience serving in Army Special Operations with multiple deployments to Iraq, Afghanistan, and the Philippines. LTC Wilcox's most recent assignment was as Director of the Afghan Local Police Special Operations Advisory Cell. As a Civil Affairs officer, he commanded 3rd Battalion, 1st Special Warfare Training Group (Airborne), A Company, 97th Civil Af-

fairs Battalion (SO)(A), and CAT 714, A Company, 97th CA Battalion (SO)(A). LTC Wilcox holds a Bachelor of Arts Degree from the Virginia Military Institute, and a Master of Science from the Naval Postgraduate School.

**LTC Sam Hayes** is an active-duty U.S. Army Civil Affairs officer serving at the 95th Civil Affairs Brigade (SO) (A). He has served with the 82nd Airborne Division, the 96th Civil Affairs Battalion, 82nd Civil Affairs Battalion, USAJFK Special Warfare Center and School, USACAPOC(A), and NATO with various deployments across the Middle East and Africa. Sam has multiple degrees to include a Master of Arts in Information Warfare and Political Strategy from Naval Postgraduate School and a Ph.D. in Organizational Management with a specialization in Leadership from Capella University.

**MAJ Assad Raza** is an active-duty U.S. Army Civil Affairs officer serving at the Western Hemisphere Institute for Security Cooperation. He has served with the 82nd Airborne Division, the 96th Civil Affairs Battalion, and the 5th Special Forces Group with multiple deployments across the Middle East. Assad holds a Bachelor of Art in psychology from the University of Tampa, a Master of Art in diplomacy with a concentration in international conflict management from Norwich University, and a Master of Military Art and Science from the U.S. Army Command and General Staff College. He is a doctoral student at Troy University in Alabama.

**NOTES** **01.** Sun Tzu *The Art of War*, trans. Samuel B. Griffith, and B. H. Liddell Hart. 1971. T (New York: Oxford University Press), 101. **02.** Joint Chief of Staff. "Competition Continuum." Joint Chief of Staff: Joint Electronic Library. Department of Defense, June 3, 2019. [https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn\\_jg/jdn\\_19.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn_19.pdf). **03.** Department of Defense, *2018 National Defense Strategy of the United States of America* (Washington, DC.: Department of Defense, January 19, 2018), <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>. **04.** Ibid, 3. **05.** Ibid. **06.** Lukas Andriukaitis, "Disinfo Bingo: The 4 Ds of Disinformation in the Moscow Protests," Atlantic Council's Digital Forensic Research Lab(blog), Medium, September 24, 2019, <https://medium.com/dfrlab/disinfo-bingo-the-4-ds-of-disinformation-in-the-moscow-protests-6624d3d677e6>. **07.** Ibid. **08.** P.W. Singer and Emerson T. Brooking, *Likewar: The Weaponization of Social Media* (Boston: Houghton Mifflin Harcourt, an Eamon Dolan Book, 2018), 206-7. **09.** Parks, Miles. "Mueller's Report Shows All The Ways Russia Interfered In 2016 Presidential Election." NPR. NPR, April 18, 2019. <https://www.npr.org/2019/04/18/714810702/muellers-report-shows-all-the-ways-russia-interfered-in-2016-presidential-electi>. **10.** Taylor, Derrick Bryson. "George Floyd Protests: A Timeline." *The New York Times*. *The New York Times Online*, May 30, 2020. <https://www.nytimes.com/article/george-floyd-protests-timeline.html>. **11.** Max Fisher and Amanda Taub, "How Everyday Social Media Users Become Real-World Extremists." *The New York Times*. *The New York Times Online*, April 25, 2018, <https://www.nytimes.com/2018/04/25/world/asia/facebook-extremism.html>. **12.** "Neither side is backing down as federal agents and protesters clash in Portland," CNN, last modified July 21, 2020, <https://www.cnn.com/2020/07/21/us/analysis-portland-protests-federal-agents/index.html>. **13.** <https://www.portland.gov/sites/default/files/2020-01/2012-vulnerability-analysis.pdf?fbclid=IwAR3KAoyP5s8Adn00Z1vQb66FjYBPsFXaRRRqZnxN29oh5jA4fK38X6RDmq0>. **14.** Ibid. **15.** United States, Department of Defense, TRADOC. (2016). ATP 5-0.6: Network Engagement. Washington, DC, DC: TRADOC. 1-7. **16.** Ibid, 1-8. **17.** Ibid, 1-13. **187.** Ibid, 1-17. **19.** Sean F. Everton, *Disrupting Dark Networks* (New York: Cambridge University Press, 2012). **20.** Nancy Roberts and Sean F. Everton, "Strategies for Combating Dark Networks," *Journal of Social Structure* 12, no. 1 (2011): pp. 1-32, <https://doi.org/10.21307/joss-2019-030>. **21.** Daniel Cunningham, Sean F. Everton, and Philip Murphy, *Understanding Dark Networks: a Strategic Framework for the Use of Social Network Analysis* (Lanham: Rowman & Littlefield, 2016). **22.** Scobell, Andrew, Edmund J. Burke, Cortez A. III Cooper, Sale Lilly, Chad J. R. Ohlandt, Eric Warner, and J.D. Williams. "China's Grand Strategy." RAND Corporation, July 24, 2020. [https://www.rand.org/pubs/research\\_reports/RR2798.html](https://www.rand.org/pubs/research_reports/RR2798.html). **23.** Bloom, Deborah. "Proud Boys Portland Rally Largely Peaceful but Clashes Downtown." Reuters. Thomson Reuters, September 26, 2020. <https://www.reuters.com/article/us-global-race-protests-portland/proud-boys-portland-rally-largely-peaceful-but-clashes-downtown-idUSKBN26H018>. **24.** Banerjee, Vasabjit. "Is the United States Heading for a Rural Insurgency?" Just Security, October 6, 2020. <https://www.justsecurity.org/72681/is-the-united-states-heading-for-a-rural-insurgency/>.



# INFLUENCE AT ECHELON

Psychological Operations in Great Power Competition.  
BY CAPTAIN PATRICK CUNNINGHAM

“Inter-state strategic competition, not terrorism,  
is now the primary concern in U.S. national security.”  
– 2018 National Defense Strategy (NDS)<sup>01</sup>

As the United States shifts focus towards great power competition, multi-domain operations, large scale combat operations and countering near-peer adversaries who have increasingly focused on rivaling our nation’s competitive advantages, the seamless integration of Psychological Operations across the conflict continuum is more critical now than ever. The United States Army Special Operations Command *Army Special Operations Forces Strategy* highlights the crucial role of PSYOP forces within its mission statement: “advancing partnerships, influencing adversarial behavior, executing special operations and responding to crisis.”<sup>02</sup> 1st Special Forces Command’s *Vision for 2021 and Beyond* recognizes PSYOP forces as unconventional warriors, masters of influence, executioners of the indigenous approach and vital members of the Army Special Operations Forces Cross-Functional Team.<sup>03</sup> The U.S. Army John F. Kennedy Special Warfare Center and School states in its approved *Psychological Operations Regimental Narrative* that PSYOP forces are experts in psychological warfare, serve as the Department of Defense’s influence capability, exploit adversary vulnerabilities and master the power of influence to shape the global security environment, impact regional stability and achieve United States national security objectives.<sup>04</sup> Throughout history and numerous large-scale operations, PSYOP forces have provided tactical, operational and strategic impact and value during competition, armed conflict and transitions back to peacetime and stability operations.

As the Army moves forward into a decisive era of inter-state, strategic competition — while simultaneously balancing requirements to counter violent extremist organizations — the

PSYOP Regiment must evolve to maintain competitive advantage against our nation’s adversaries. To succeed, we must exhibit agile and adaptive leadership, a deep hunger for innovation and creative solutions to complex problems and a relentless drive to shatter the status quo — challenging the realms of what is possible and what is not. To remain competitive in 21st Century GPC, defend the free world and democratic ideals and set conditions to win in war, the PSYOP Regiment must excel in three specific focus areas: Employing information warfare at scale, persistent engagement through cyberspace and aggressive network development to support unconventional warfare and irregular warfare objectives.

## CONCEPTUAL IMPLEMENTATION THROUGHOUT AMERICAN HISTORY

### American Revolution

American Psychological Warfare has many vignettes and historical examples to illustrate the successes and effects achieved when information warfare, persistent engagement and aggressive network development are synchronized. While cyberspace was not a warfighting domain until the cusp of the 21st century, the concept of persistent engagement through emerging technology and innovative practices remains constant. Samuel Adams was one of the American Revolutions’ most prolific writers, leveraging the printing press as the technological innovation of the time to manage multiple pen names and even going so far as to change his writing style to fit the pen name.<sup>05</sup>

### World War II

In World War II, the Office of Strategic Services — the direct precursor to the Central Intelligence Agency and Special Operations Forces — established the Morale Operations Branch, designed to clandestinely “influence enemy thinking by means of black propaganda... that would appear as though it had come from within the enemy’s own ranks.” The MO Branch leveraged networks of proxy forces and agents to dissem-

inate forged newspapers and military orders, operate clandestine transmitters that appeared to be broadcasting from within enemy territory and initiated rumor campaigns — many of which permeated to such an extent that allied intelligence confirmed that they impacted senior axis leadership decision making.<sup>06</sup>

John Steinbeck — the legendary American author best known for *Grapes of Wrath* — assisted the OSS's Office of War Information during World War II and authored *The Moon is Down*, one of the most far reaching PSYOP products in Western Europe. *The Moon is Down* chronicles a “Norwegian-based” resistance organization from inception to employment, tacitly instructed northern Europeans on how to develop UW campaigns, sabotage and subvert Nazi war efforts and invigorated numerous countries under Axis invasion to build comprehensive auxiliary, underground and guerilla forces. During the armed conflict of World War II, the novel was translated and printed on clandestine presses, and disseminated across Norway, Denmark, Holland and France. *The Moon is Down* was so effective in empowering resistance that since 1942, more than 92 translated editions have appeared across 28 countries. More than just a compelling work of art, the success of *The Moon is Down*

epitomizes the synchrony of leveraging emerging technology, information warfare principles, persistent engagement across multiple fronts against adversaries and aggressively developing and utilizing friendly networks.<sup>07</sup>

### Cold War to the Present Day Global War on Terror

Numerous vignettes of synchronized information warfare at scale, persistent engagement and aggressive network development exist from the onset of the Cold War, through the Global War on Terror and up to present day efforts to outcompete and impose cost against our adversaries. Project Eldest Son was a joint effort between the CIA and SOF to sabotage Viet Cong weapons caches with exploding ammunition for lethal and psychological effects. As part of a larger military deception effort, Project Eldest Son eroded Viet Cong confidence in their weapons systems and trust in their chain of command. Recent campaigns in Afghanistan and Syria have mirrored this effort with commensurate effects.<sup>08</sup> Numerous PSYOP campaigns were carried out against ISIS and other terrorist organizations across Afghanistan, Iraq and Syria that focused on increasing desertion and internal rifts, decreasing morale, synchronizing friendly networks to reduce public and auxiliary support to ISIS fighters,

and denying safe havens to violent extremist organizations.<sup>09,10,11</sup>

In Trinidad and Tobago, the highest per-capita recruiting ground for the western hemisphere, a PSYOP team employed radio, television and print products to elicit public denouncements of ISIS and VEOs. The PSYOP team worked closely with Special Forces elements and a Civil Affairs team, while collaborating with U.S. Embassy personnel and partner nation influencers to develop culturally and psychologically significant community events to strengthen resistance efforts against VEO recruiting. ARSOF worked to create an environment that was inhospitable to violent extremism and Salafi Jihadism across Trinidad, by uncovering terrorist networks and promoting regional stability alongside our nation's Caribbean allies.<sup>12</sup>

## INFORMATION WARFARE AT SCALE

There is no codified or doctrinal definition for information warfare. However, for the purposes of this paper, “information warfare at scale” refers to the fusion of large-scale influence operations that focus on the mobilization or demobilization of mass populations, surgical influence operations and psychological warfare to effect critical nodes within the multi-domain battlespace, with coordinated information-related

Figure 01  
This Operational Approach captures the author's view on how to best posture the PSYOP Regiment to mature and excel in 21st century Great Power Competition.

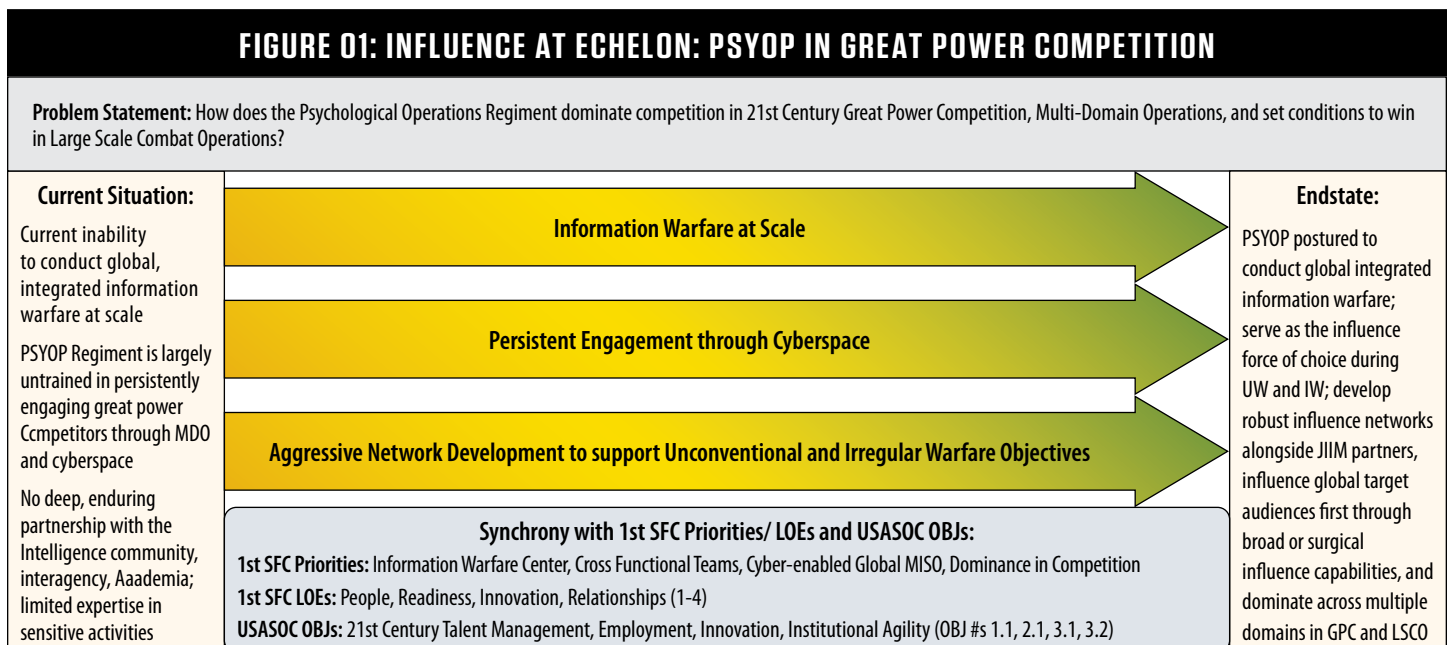
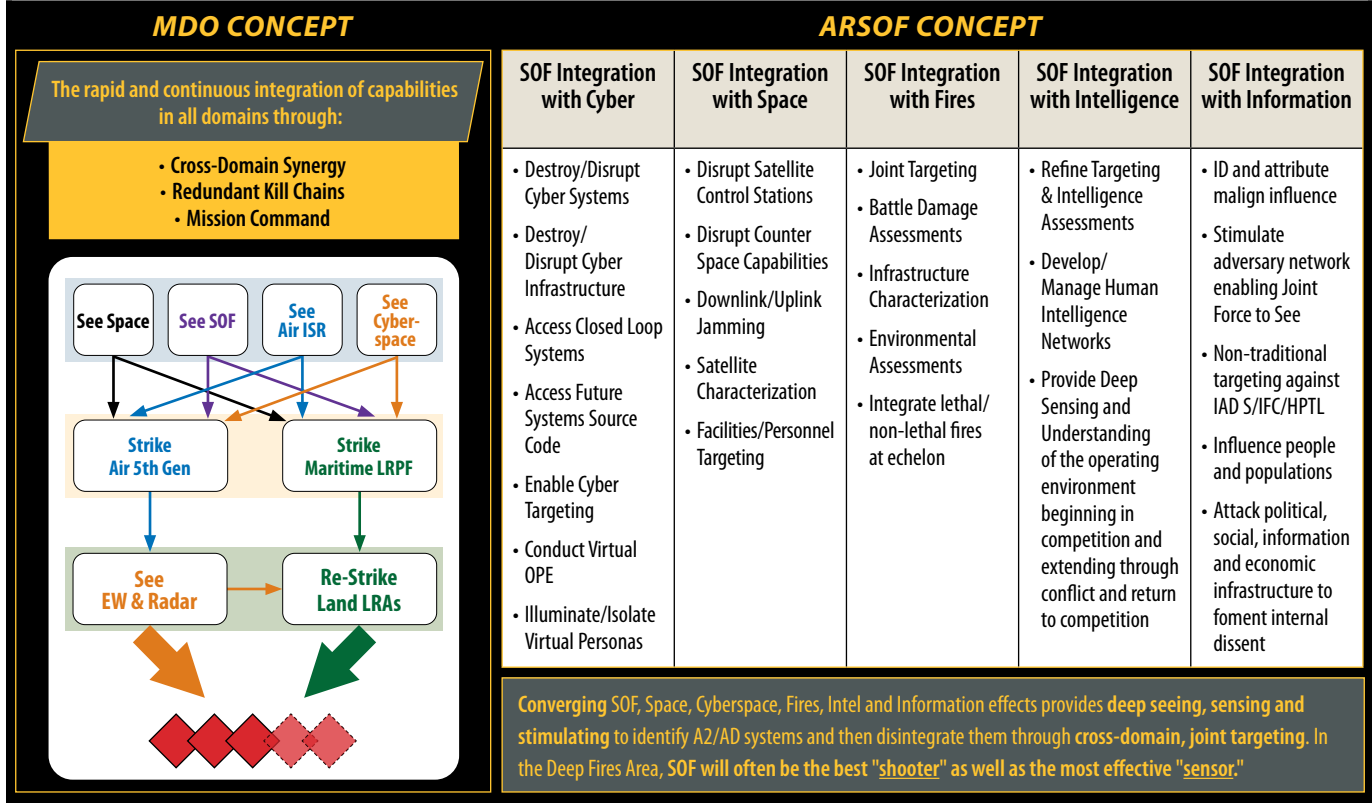


Figure 01

**FIGURE 02: ARMY SPECIAL OPERATIONS ROLE IN MULTI-DOMAIN OPERATIONS**



capabilities for tactical, operational and strategic effects. U.S. Army Cyber Command defines information warfare as “a developing concept for competing and defeating adversaries in the information environment and cyberspace domain. It includes the employment of military capabilities, under military authorities, to generate deliberate effects in the cognitive, physical and informational dimensions of the information environment in support of multi-domain campaigns.” Operations against ISIS, disrupting Russian attempts to interfere in the 2018 U.S. midterm elections and, most recently, countering Iran’s attempts to increase instability across the Middle East mark important efforts by the U.S. military to find effective capabilities, doctrinal concepts and appropriate roles in an era of information warfare.

Information warfare and PSYOP can occur across the competition continuum, from conflict and deterrence to large-scale combat operations, including UW and IW campaigns that will increasingly dominate the future of GPC. Information warfare and PSYOP are especially critical

throughout the seven phases of UW. “Psychological preparation to unify the population against the established government or occupying power and prepare the population to accept U.S. support” is the basis of Phase I: Preparation, and as ARSOF forces conduct initial contact and infiltration, aggressive MILDEC and delegitimization of the adversarial government is necessary for the respective protection of friendly forces and development of indigenous support. During Phase IV: Organization, and Phase V: Buildup, PSYOP forces can surge clandestine recruiting efforts and partner with covert influence assets to synchronize Title 10 and 50 authorities, leverage 3rd Psychological Operations Battalion (Airborne) for appropriate influence products and translated resistance training manuals; and synchronize Space, Cyber and Electronic Warfare assets to obfuscate, degrade or destroy adversarial sensor or targeting mechanisms — even injecting messages into adversarial communications platforms for maximum psychological impact. During Phases VI and VII (Employment and Transi-

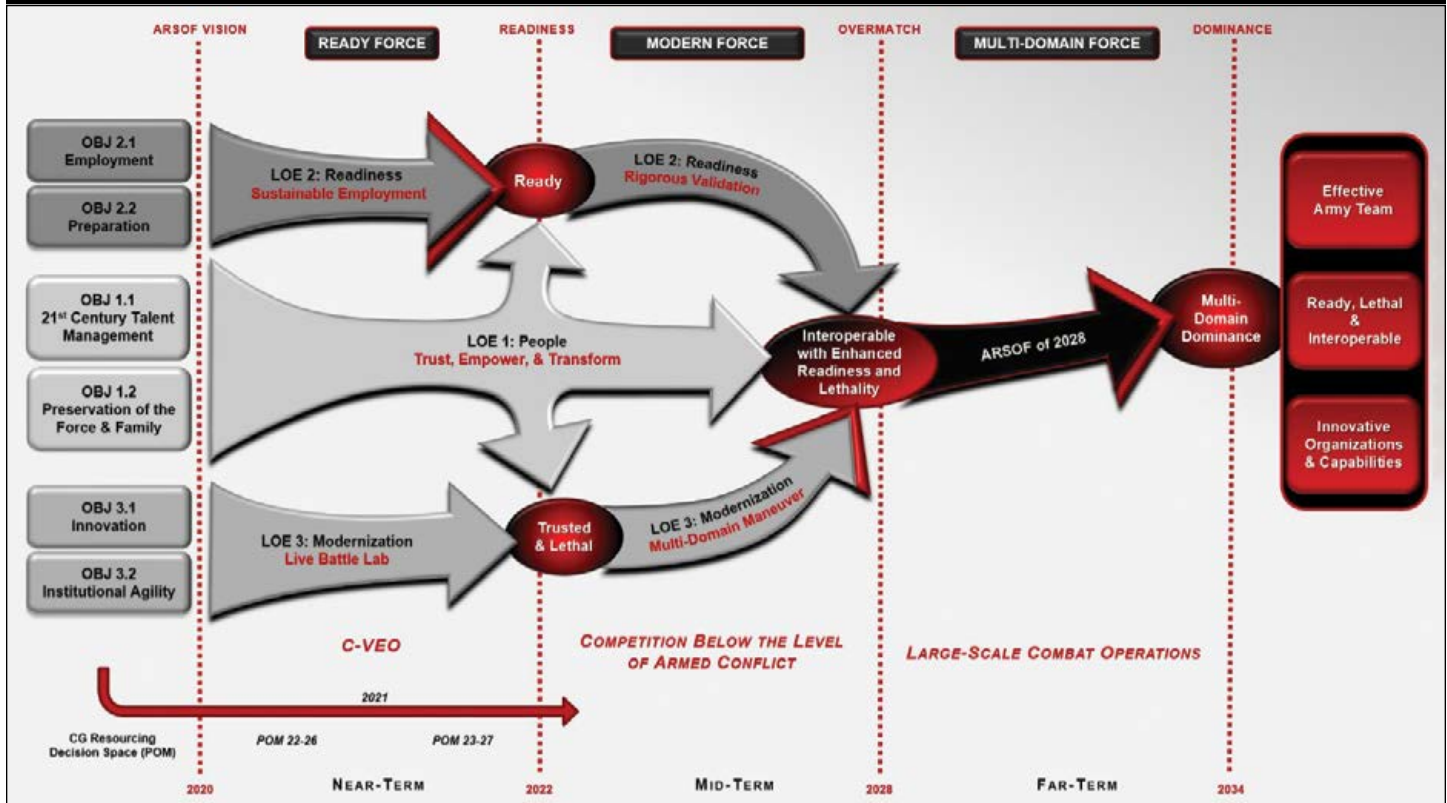
tion), clandestine, regionally focused, international and surgical cyber-enabled influence operations intensify; Space, Cyber and EW assets converge for adversarial communication denial and anti-access area denial node destruction or severe degradation; and international condemnation of adversarial crimes against humanity and human rights violations and calls for a peaceful transition to the new government can be increased and amplified through Department of State or Public Affairs key influencers.

The *Joint Concept for Human Aspects of Military Operations* echoes the criticality of coordination information warfare at scale from a Joint Perspective. JC-HAMO explains that during LSCO:

*“The Joint Force and its partners must defeat the enemy, but also make peace attractive. They must strive for military supremacy, yet also demonstrate the benefits of their cause. The destruction of an adversary’s entire military capacity is almost never feasible and doing so without political solutions*



**FIGURE 03: ARSOF STRATEGIC APPROACH (FROM USASOC ARSOF STRATEGY)**



may lead to a regeneration of the armed conflict by personally and ideologically motivated actors. Consequently, the joint force must find ways to degrade an adversary's resolve and legitimacy. The choice of what to target and when to strike must consider the desired psychological and political effect. The Joint Force and its partners must consider, for example, if their intent is to weaken, degrade or destroy an adversary — or create some other desired effect.”<sup>13</sup>

In terms of information warfare organizational operational scaling, the recently developed Information Warfare Task Force construct presents an operationally effective mechanism of executing IWS. From 2017, the ARSOF community developed and led Information Warfare Task Force-Afghanistan during combat operations. The IWTF-A was formed in theatre to focus on achieving cognitive effects through the synchronized employment of maneuver forces

and influence activities. Leveraging hostile fire zone authorities, IWTF-A employed PSYOP forces, publicly available information collection tools, data-analytics capabilities, robust Intelligence capabilities and cutting-edge digital advertising technology to deliver highly effective influence messaging.<sup>14</sup> The success of IWTF-A in disrupting and degrading both ISIS-K and the Taliban spurred development of other IWTF or IWTF-like constructs.<sup>15</sup>

Namely, IWTF-IP was established in the USINDOPACOM AOR to counter Chinese influence efforts, aggressive expansionism and defend democratic ideals; IWTF-C was established in the USCENTCOM AOR to counter Iranian Threat Networks, and the Information Warfare Center was established at Fort Bragg to serve as a CONUS-based IWTF-like enterprise that conducts persistent, global, integrated information warfare remotely to monitor networks, identify and characterize adversary activities and vulnerabilities and employ integrated global information warfare, in collaboration with Joint

Interagency Intergovernmental Multinational partners and the greater ARSOF network to disrupt, deny, degrade and influence NDS priority threats across the competition continuum.<sup>16,17</sup>

PSYOP forces must be the forefront of layering, executing and penetrating denied space with influence operations at echelon, despite the capability of a near-peer adversary employing systems designed to disrupt the integration of the Joint Force and degrade exquisite capabilities. Developing an agile, cloud-based common operating picture that leverages artificial intelligence and machine learning for tracking, directing and understanding information warfare at scale and adversarial actions, as well as an ability to provide Internet in denied areas to enable ARSOF to wield influence will become critical in the very near future. Doing so will enable PSYOP forces to reach local populations, indigenous forces, resistance forces, shadow governments and other foreign target audiences in support of efforts to inform, persuade direct,

deceive, confuse and/or disrupt. Most critically, these capabilities would also enable ARSOF to counter adversarial influence; conduct virtual train, advise and assist; military source operations, and many other virtual aspects of UW and cyber-enabled military information support operations in support of 21st century information warfare.

### PERSISTENT ENGAGEMENT THROUGH CYBERSPACE

Mastery of Cyber-enabled MISO and information warfare is absolutely critical to the advancement of the PSYOP Regiment in 21st century GPC. While the vast majority of specific details regarding cyber-enabled information warfare can only be provided at a top secret level, and to a much lesser extent, at the secret level, the speed, agility and surgical influence capability against near-peer threats is truly incredible and will actively shape the future of our nation's wars and executing MDO.

General Clarke, the U.S. Special Operations Command Commander stated that "winning the fights of the future" will "depend more on tech-savvy operators trained for the Cyber and Information battlespace," that it will be "increasingly important for SOF to operate in the non-physical information space," and that he is convinced that "working in the information space can have the greatest impact in the coming years."<sup>18</sup> Leveraging Cyber assets to execute surgical PSYOP allows ARSOF to serve as the Army force of choice for dominating in competition, defeat adversary attempts to expand the competitive space, deter escalations of violence and strike in the virtual and cognitive realms of the deep maneuver and deep fires areas to create second fronts that present multiple dilemmas.<sup>19</sup> Aggressive development towards actualizing PSYOP mastery of Cyber-enabled influence also epitomizes the 1st SFC culture of "constant innovation and improvement," forges next generation leaders who "excel in ambiguous environments, overcome challenging conditions, influence and win, whether on the battlefield, online

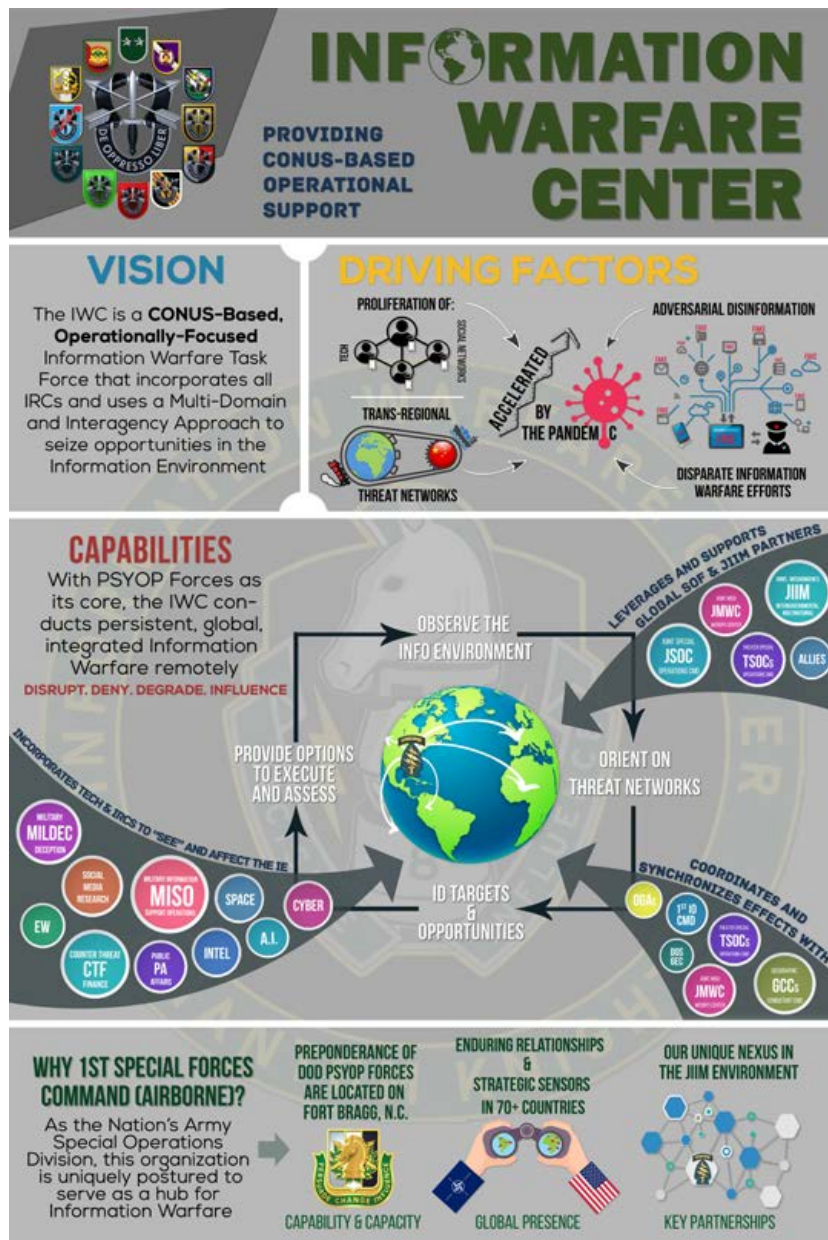


Figure 04

or in competition with our collective adversaries," and enables 1st Special Forces Command PSYOP personnel to develop Cyber-focused career pathways — as outlined in *1st SFC(A) Force Development and Resource Management* manning guidance.<sup>20,21</sup> More than just a choice, excelling in "Cyber-Enabled Global MISO" and information warfare is the duty and specific innovation focus area that 1st Special Forces Command has entrusted to 8th Psychological Operations Group to excel in and innovatively lead change.<sup>22</sup>

"Imposing Cost" upon NDS-threat aligned foreign adversaries has been a key tenant of the IWC's design theory and operational functions, although the aperture of this focus should include "persis-

tent engagement" as well. The term "Impose Cost" is connotative of *quid pro quo* – executing a U.S. action in response to an adversarial action. However, our adversaries attempt to attack our intellectual property, financial institutions, democratic processes, operational plans, and service members on a daily basis. China aggressively pushes the limits of what they can get away with in terms of intellectual property theft and siphons an estimated \$600 billion per year in terms of stolen information from the U.S. No direct U.S. action prompted this, merely China's unscrupulous desire to create a new-world order where China rules and autocratic regimes outcompete democratic nations.<sup>23</sup> Russia

has employed “little green men” as part of an illicit hybrid warfare campaign to illegally seize terrain in Ukraine and Georgia, launched vicious Distributed Denial of Service attacks against our allies in the Baltics,<sup>24</sup> Iran continues to leverage proxies and surrogates to destabilize the Middle East, North Korea aggressively pursues nuclear weapon accumulation while evading U.S. sanctions through cryptocurrency exploitation, and VEOs continue to strike where they can for territorial or ideological gain.<sup>25</sup> PSYOP forces must get ahead of these threats by not merely “imposing cost” but also employing “persistent engagement” through Cyberspace in concert with social media, traditional media and face-to-face engagements.

Historically, Regional PSYOP Teams, Military Information Support Teams and Tactical PSYOP Teams have been “Imposing Cost” against VEOs and NDS-aligned threats as a means of countering adversary influence, limiting adversarial operational effectiveness, degrading popular support for the adversary and/or enabling and enhancing both lethal and non-lethal targeting and strikes. Executing influence operations “by, with, and through” PN or indigenous forces has enabled ARSOF to shape the operational environment in our

favor, and in line with strategic U.S. objectives. Cyber persistence theory argues that since the potential for exploitation is ever-present in cyberspace, and since states are in constant contact due to interconnectedness, states must assume their sources of national power are vulnerable. The strategic principle of seizing the initiative is the essence of persistent engagement. Understanding states’ Cyber behaviors as *faits accomplis* bolsters the argument for adopting a cyber-enabled information warfare strategy of persistent engagement, which anticipates the unilateral actions of aggressors and sets the conditions of security in favor of U.S. objectives.<sup>26</sup>

U.S. Cyber Command’s initiative to exploit vulnerabilities in the Cyber infrastructure of the Internet Research Agency in Russia to defend the 2018 U.S. midterm elections is an example of this concept in action. Many more examples exist at higher

levels of classification. While USCC is already acting to anticipate and address vulnerabilities, there is room for improvement. USCC has recruited and hired legions of technological experts for the Cyber Domain, but they have not recruited for expertise in PSYOP. Lt. Gen. Stephen Fogarty, commander of ARCYBER, noted that “sometimes, the best thing I can do on the Cyber side is actually to deliver content, deliver a message... Maybe the cyberspace operation I’m going to conduct actually creates some type of [PSYOP] effect.”<sup>27</sup>

The PSYOP Regiment must be postured to leverage Cyber assets, compromised adversary networks, and use specific, surgical capabilities to deliver influence effects. Influencing adversarial decision makers, workers, militaries or various demographics to contribute to the reporting and mapping of A2AD nodes, critical infrastructure, or network degradation all lead to

01  
A PSYOP leaflet designed to target members of ISIS to encourage desertion from the group in order to weaken it. Historically, PSYOP have been “Imposing Cost” against adversary threats as a means of countering influence, limiting adversarial operational effectiveness, degrading popular support for the adversary, and/or enabling and enhancing both kinetic and non-kinetic targeting and strikes.

**Front translation:** “Coalition pilots prowl the skies. Listen for their roar and look for the fire and smoke that signifies another [ISIS] has been sent back to Barzakh.”

*In Islamic theology, Barzakh is believed to be an intermediate location between the physical and the spiritual worlds where deceased individuals have time to contemplate their worldly actions before final Judgment Day and entry into eternity.*

**Back Translation:** “Committing atrocities against innocent citizens is cowardly and unforgivable. [ISIS] have corrupt souls and will see Jahannam. Abandon your illegitimate cause.”

*In Islamic theology, Jahannam signifies Hell.*



01

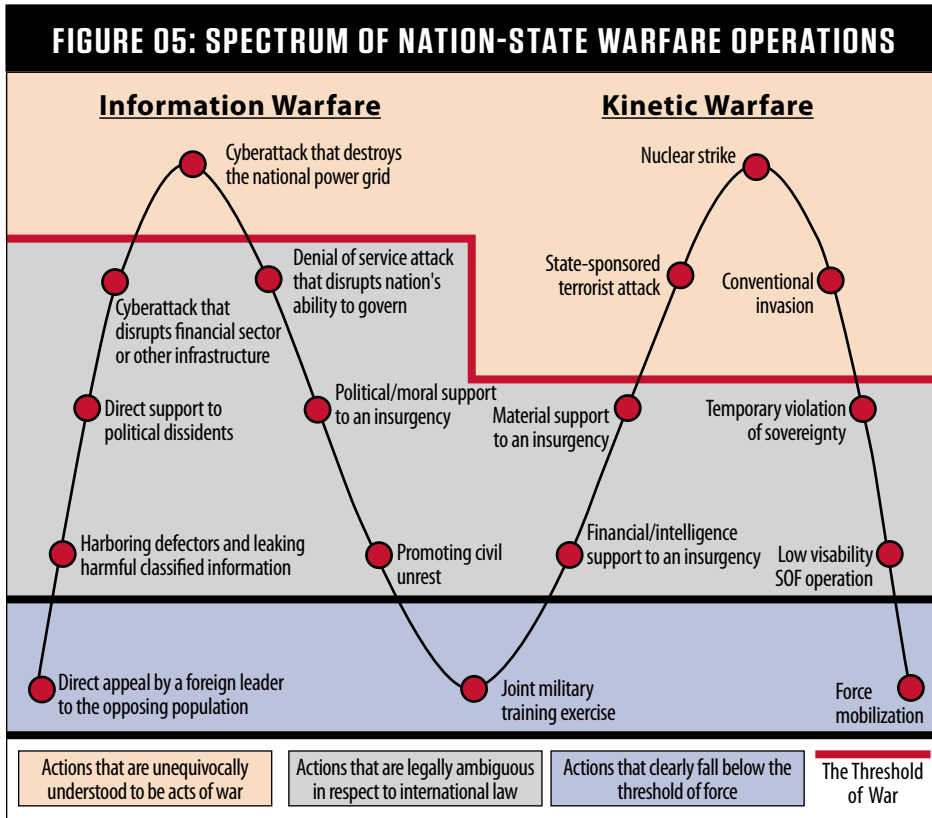


Figure 05  
A visual depiction highlighting the spectrum of Nation-State Warfare Operations, and a useful tool to visualize the 21st Century Unconventional, Irregular, and Information Warfare conflict continuum.

an optimized “kill chain” or “A2AD node disruption chain” that change adversary decision calculus and allow the USG and partner forces to impose multiple, chaotic, dilemmas upon the adversary.

### AGGRESSIVE NETWORK DEVELOPMENT TO SUPPORT IRREGULAR WARFARE OBJECTIVES

Thirdly, PSYOP forces must be postured to leverage friendly networks across multiple domains to achieve Irregular Warfare Objectives. In addition to deploying forward and executing influence operations by, with, and through PN key influencers, key communicators, and PSYOP counterparts, PSYOP must be closely integrated with Sensitive Activities organizations, the Intelligence Community, Interagency, academia, and industry. Beyond leveraging proxy and surrogate forces, and collaborating with the agencies and organizations that employ them, the PSYOP Regiment must also focus on maintaining forward deployments in significant locations, and deepening relationships with

academia, the IC, and IA partners to outcompete global adversaries.

Deploying forward to tactically, operationally, and strategically significant locations will always need to be a priority for the PSYOP Regiment in GPC, because it enables ARSOF PSYOP forces to act as key sensors in deployed environments and truly serve as the “first to influence.” Forward deployed PSYOP elements are critical assets that can provide the “ground truth” on friendly, indigenous, and adversarial influence capabilities and ongoing efforts, identify adversary propaganda and generate shared understanding across U.S. Embassy Leadership and Theatre Special Operations Command, physically enable the dissemination of influence products and engage Key Leaders, PN forces and local influencers to modify and change their behavior to support U.S. objectives. Additionally, in environments where media capabilities are contested or controlled by the adversary, forward deployed PSYOP forces are critical assets to UW and IW campaigns by identifying influential human beings who can carry messages and products forward in a clandestine

manner, amplify recruiting efforts, clandestinely sabotage A2AD nodes, and elicit international condemnation of adversarial crimes against humanity and human rights violations, and calls for a peaceful transition to the new government.

Partnering with Clandestine influence partners will also become increasingly important for the PSYOP Regiment in the 21st century. Deepening relationships and collaborative efforts with the Defense Intelligence Agency’s Defense Clandestine Service, CIA’s Covert Influence section, and Federal Bureau of Investigation Human Intelligence sections, can lead to a significant, “mutually reinforcing” approach regarding the complementary nature of Title 10 and Title 50 authorities, by leveraging appropriate Intelligence partners and authorities to influence an environment and shape it favorably to U.S. objectives.<sup>28</sup> This partnership naturally supports and amplifies the DoD’s Operational Preparation of the Environment, part of which includes the Psychological Preparation of the Environment to set conditions for future actions by the SOF community or conventional forces at large. Synchronizing efforts with the 1st SFC Office of Special Warfare facilitates the PSYOP Regiment’s contribution to the SA realms of warfare, which will become even more necessary in conducting clandestine operations, facilitating A2AD node disintegration, creating chaotic dilemmas for the adversary minimizing the U.S. footprint while maximizing effects and setting conditions to enable a rapid transition to armed conflict.

Furthering the PSYOP Regiment’s coordination and collaboration with USCC and other members of the Signals Intelligence, Open Source Intelligence, and aforementioned members of the HUMINT Communities will dramatically enhance our ability to conduct Information Warfare at Scale through MILDEC and Cyber-enabled Global MISO and Information Warfare. USCC has proven an incredible asset in delivering surgical influence packages against near-peer threats, and has assisted the PSYOP Regiment in understanding how


our adversaries utilize cyberspace as a warfighting domain. Deepening partnerships with our robust IC as a mechanism to “Integrate with U.S. interagency” is directed by the most recent NDS and will prove pivotal in countering adversary coercion and subversion.<sup>29</sup> In addition to directly supporting the NDS’s Strategic Approach and *1st SFC Vision for 2021 and Beyond*, deepening IC partnerships will posture the PSYOP Regiment to contribute exponentially to SA and cyber-enabled Global MISO while producing expertise in non-traditional and critical functional career pathways.<sup>30, 31</sup>

Academia offers numerous opportunities for symbiotic collaboration, and is for the most part, a massively untapped resource. Partnership and collaboration with Johns Hopkins University Applied Physics Laboratory, for example, has historically been intermittent but presents an incredible opportunity for the PSYOP Regiment to spearhead transformative innovation efforts that allow USASOC as a whole to better understand the IE and weaponize information. JHU-APL, and academic partnerships writ large, posture the PSYOP Regiment to challenge the status quo regarding how we conduct influence operations, secure a foothold in academia to increase responsiveness to evolving needs, expand 1st SFC’s clandestine influence apparatus, and establish a mutually beneficial nexus between the IWC, Cyber National Mission Force, various influence-focused agencies in the National Capital Region. JHU-APL is an epicenter of innovation and modernization, aggressively pursues influence superiority against our adversaries, and is actively shaping how data collection, AdTech utilization, network analysis and influence operations are conducted in the 21st century. Critically, numerous leaders within JHU-APL are eager to begin working with 8th POG(A) in three primary facets: Low to No Cost Training on a variety of computer science and analytic competencies, Robust Information Sharing and Acting as a Strategic Nexus between the PSYOP regiment, academia,

CNMF/ USCC, the IC and Sensitive IA Partners. We cannot afford to let this opportunity, or those that exist to enable the USASOC Objectives of Innovation and Institutional Agility, pass us by.<sup>32</sup>

## CONCLUSION

As the Army and our nation continue to move forward into a decisive era of inter-state, strategic competition, the PSYOP Regiment must evolve in order to maintain competitive advantage against our Nation’s adversaries. Through the methodical synchronization and employment of information warfare at scale, persistent engagement through Cyberspace, and aggressive network development to support UW and IW Objectives, PSYOP forces will become increasingly convergent and remain at the leading edge of GPC, MDO, and LSCO.

By “powering down authorities” to enable decisive Information Warfare and cyber-enabled Influence Operations, partnering and engaging persistently through cyberspace, and aggressive network development, PSYOP forces will be able to better expand physical access and influence, leverage a robust network of JIIM partners and surrogates to produce effects against adversaries in complex, austere, and sensitive environments, and operate alongside the National Mission Force, IA, and IC partners to execute discreet SA in support of national objectives. Synchronization and mastery of these three basic principles will yield unprecedented results in the PSYOP Regiment, forge more lethal and agile ARSOF CFTs, posture 1st SFC and USASOC achieve dominance in the competition space against global threats, truly enable Influence at Echelon, and shatter the status quo of what is considered possible. 

## ABOUT THE AUTHOR

**CPT Patrick Cunningham** is an active duty Army Psychological Operations officer, assigned to the 8th Psychological Operations Group (Airborne).

**NOTES** **01.** Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military’s Competitive Edge, (Washington, DC: Department of Defense, 2018), 1. **02.** United States Army Special Operations Command Army Special Operations Forces Strategy (Fort Bragg, NC: United States Army Special Operations Command, 2019), 2. **03.** *1st Special Forces Command (Airborne) Vision for 2021 and Beyond*, (Fort Bragg, NC: 1st Special Forces Command, 2020), 2-6. **04.** *Psychological Operations Regimental Narrative*, (Fort Bragg, NC: United States Army John F. Kennedy Special Warfare Center and School, 2017), 2. **05.** Martin J. Manning, Clarence R. Wyatt, eds., *Encyclopedia of Media and Propaganda in Wartime America: Volume I* (Santa Barbara: ABC-CLIO, 2011), 7. **06.** Richard Harris Smith, *DSS: The Secret History of America’s First Central Intelligence Agency*, (Guilford, CT: Lyons Press, 2005), 11. **07.** Donald V. Coers, “Introduction,” John Steinbeck, *The Moon is Down* (New York, Penguin Books, 1995). **08.** C. J. Chivers, “Syrians Place Booby-Trapped Ammunition in Rebel’s Guns,” *New York Times*, October 19, 2012, [https://www.nytimes.com/2012/10/20/world/middleeast/syrian-government-booby-traps-rebels-ammunition.html?pagewanted=all&\\_r=0](https://www.nytimes.com/2012/10/20/world/middleeast/syrian-government-booby-traps-rebels-ammunition.html?pagewanted=all&_r=0). **09.** Jared M. Tracy, PhD., “MISTF-C in Operation Inherent Resolve,” *Veritas*, Vol. 13, No. 1, 2017. **10.** Jared M. Tracy, PhD., “The Voice of Gizab: Tactical Radio Support to Village Stability PSYOPs, civil affairs ‘sets and reps’ in messaging and setting up local governance, three-star says,” *Army Times*, October 25, 2019. **12.** 8th Psychological Operations Group (Airborne), “PSYOP Stories – Episode 2,” produced by 8th Psychological Operations Group (Airborne), *PSYWAR*, November 9, 2020. <https://youtu.be/D17u5YnKjz8> **13.** General Paul J. Selva, *Joint Concept for Human Aspects of Military Operations*, October 19, 2016, 23. **14.** Lieutenant General Stephen G. Fogarty, Colonel (Ret.) Bryan N. Sparling, “Enabling the Army in an Era of Information Warfare,” *Cyber Defense Review*, (West Point, NY: Army Cyber Institute, Summer 2020) 1-23. **15.** NATO Special Operations Component Command – Afghanistan / Special Operations Joint Task Force – Afghanistan, “Convergence and Overmatch in the Cognitive: Lessons Learned from Information Warfare Task Force – Afghanistan (IWTF-A),” White Paper, (Bagram Airfield, Afghanistan: April 6, 2020). **16.** COL Jeremy S. Mushtare, “IWC Mission,” (Fort Bragg, NC: 8th Psychological Operations Group, 19 July 2020). **17.** 1st Special Forces Command Public Affairs Office, “Information Warfare Center Infographic,” (Fort Bragg, NC: 1st Special Forces Command, 10 August 2020). **18.** Matthew Cox, “Less Door-Kicking, More Influencing: The Changing Role of Special Operators,” *Military.com*, 12 May 2020, <https://www.military.com/daily-news/2020/05/12/less-door-kicking-more-influencing-changing-role-special-operators.html>. **19.** *US Army Special Operations Command (Airborne) Army Special Operations Forces Strategy*, (Fort Bragg, NC: US Army Special Operations Command, 2019), 3. **20.** *1st Special Forces Command (Airborne) Vision for 2021 and Beyond*, (Fort Bragg, NC: 1st Special Forces Command, 2020), 4. **21.** *1st Special Forces Command (Airborne) Force Development & Resourcing Guidance (Draft)*, (Fort Bragg, NC: 1st Special Forces Command, 2020), Introduction: VI. **22.** *Ibid*, X. **23.** Jim Sciutto, *The Shadow War: Inside Russia’s and China’s Secret Operations to Defeat America*, (New York, NY: HarperCollins Publishers Ltd., 2019), 72-78. **24.** *Ibid*, 25. **25.** David Kilcullen, *The Dragons and the Snakes: How the Rest Learned to Defeat the West*, (New York, NY: Oxford University Press, 2020), 18-69. **26.** Dr. Michael Fischerkeller, “The Fait Accompli and Persistent Engagement in Cyberspace,” *War on the Rocks*, June 24 2020, <https://warontherocks.com/2020/06/the-fait-accomplis-and-persistent-engagement-in-cyberspace/>. **27.** Herb Lin, “On the Integration of Psychological Operations with Cyber Operations,” *Lawfare*, January 9 2020, <https://www.lawfareblog.com/integration-psychological-operations-cyber-operations>. **28.** Michael E. DeVine, “Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions in Brief,” (Washington, DC: Congressional Research Service, 14 June 2019), 1-8. **29.** Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military’s Competitive Edge, (Washington, DC: Department of Defense, 2018), 5. **30.** *1st Special Forces Command (Airborne) Force Development & Resourcing Guidance (Draft)*, (Fort Bragg, NC: 1st Special Forces Command, 2020), Introduction: VII. **31.** *1st Special Forces Command (Airborne) Vision for 2021 and Beyond*, (Fort Bragg, NC: 1st Special Forces Command, 2020), 5. **32.** Patrick Cunningham, “Johns Hopkins University Applied Physics Laboratory Executive Summary,” (Fort Bragg, NC: 8th Psychological Operations Group, 06 November 2020), 1-3.



# THE LOOMING THREAT OF SYNTHETIC MEDIA

BY CAPTAIN BENJAMIN J. LEVINE

**“Artificial intelligence is the future, not only for Russia, but for all mankind...Whoever becomes the leader in this sphere will become the ruler of the world.”**

— *Russian President Vladimir Putin*

## INTRODUCTION

“In contrast to the West,” writes Clint Watts, a Non-Resident Fellow at the Alliance for Securing Democracy, “Russia does not see information warfare as a separate or even a secondary effort in pursuit of its foreign policy goals.”<sup>02</sup> Instead, he continues, it “guide[s] the Kremlin’s strategic approach to defeating the West.”<sup>03</sup>

The seriousness with which Russia approaches information warfare cannot be understated and it must be met with an appropriately calibrated response. As will be discussed, disinformation is a critical aspect of Russia’s strategy that shapes the great power competition. While it is already of great import today, it will take on even greater significance in the near future. A factor in this increased significance, although certainly not the only one, is the exponential speed at which artificial intelligence is developing. There is no doubt that AI will continue to shape the information environment in the years to come, redefining old challenges and presenting entirely new ones not yet known. This article is concerned with one key element of AI vis-à-vis the IE and Russian information warfare: synthetic media and deepfakes.<sup>04</sup>

The chief aim of this article is to direct attention toward synthetic media and disinformation, specifically regarding Russian information warfare and the danger it poses to American national security. To accomplish this, there will be a wide array of information covered herein. The first part of the article will be broken into three parts: a brief history of synthetic media, a simplified look at how the technology works, and an analysis of the psychological, technical and sociological factors that contribute to the seriousness of the threat. The second part of the article will cover the history of Russian disinformation, how the Kremlin will leverage synthetic media in the future, and how this impacts the GPC. Finally, recommendations will be offered as to what the United States can do to prepare for this looming threat.

## THE RISE OF SYNTHETIC MEDIA AND THE UNIQUENESS OF THE THREAT

### *The GANfather*

While out for drinks with fellow doctoral candidates at a bar in Montreal in 2014, Ian Goodfellow inquired if his peers would be interested in taking up a project with him: the development of a system that could produce wholly AI generated media.<sup>05</sup> Other researchers in the AI field were already trying this. However, their systems produced photos that were generally subpar and crude, immediately sus-

ceptible to detection by the most disinterested of observers.<sup>06</sup> At any rate, Goodfellow was not interested in copying these approaches. What he had in mind differed drastically.

The projects at the time were certainly impressive, using neural networks — “algorithms loosely modeled on the web of neurons in the human brain”<sup>07</sup> — and intricate machine learning frameworks, yet Goodfellow wondered if a seemingly impossible advancement was, in fact, not entirely out of the question: What would happen if you took two neural networks and made them compete *against* each other? What began as an interesting proposition over beers resulted in an innovation that would change AI in a markedly revolutionary manner: the Generative Adversarial Network.<sup>08</sup> Goodfellow would from then on be known colloquially as the GANfather.

### *The Process*

In order to understand the threat, there must first be a basic understanding of the process and technology underpinning it. GAN’s can be broken into the three parts of its name: generative, adversarial and networks. The generative aspect refers to the unsupervised learning framework of the machine, which takes large quantities of data as input and then outputs similar data (hence, generative). They are adversarial in the sense that they pin two networks against each other, which also accounts for the network descriptor.<sup>09</sup>

GAN’s are exactly what Goodfellow had imagined they would be that night at the bar: two neural networks, a generator and a discriminator (or detector), competing against each other in a technological tug-of-war match. In simple terms, this is how a GAN functions relative to developing synthetic photography, for example: one network attempts to detect artificially generated photos produced by the other, while the network producing the photos attempts to fool the detecting network (which

PHOTOS LEFT

**Fake people generated entirely via artificial intelligence using an algorithm known as the generative adversarial network.** PHOTOS CREATED BY THISPERSONDOESNOTEXIST.COM

works to improve its detection capability every iteration). These competing networks go back and forth until a product is created that cannot be detected as synthetic, although it most certainly is.

Goodfellow had pioneered a remarkable development in AI. While deep-learning machines had been quite good at *recognizing* things, they were now capable of *creating* things in an unsupervised learning framework.<sup>10</sup> Of the countless innovations in AI, this particular breakthrough was still uniquely consequential.

### The Democratization

The democratization of the GAN unfolded, in part, in the dark corners of the Internet. In December of 2017, a disturbing video emerged online. It purported to feature Gal Gadot, the famous Israeli actress, having sex with her stepbrother. However, this was *not* Gadot. While the quality of the video was imperfect — there were glitches that revealed its altered nature — to the casual observer, it passed unnoticed.

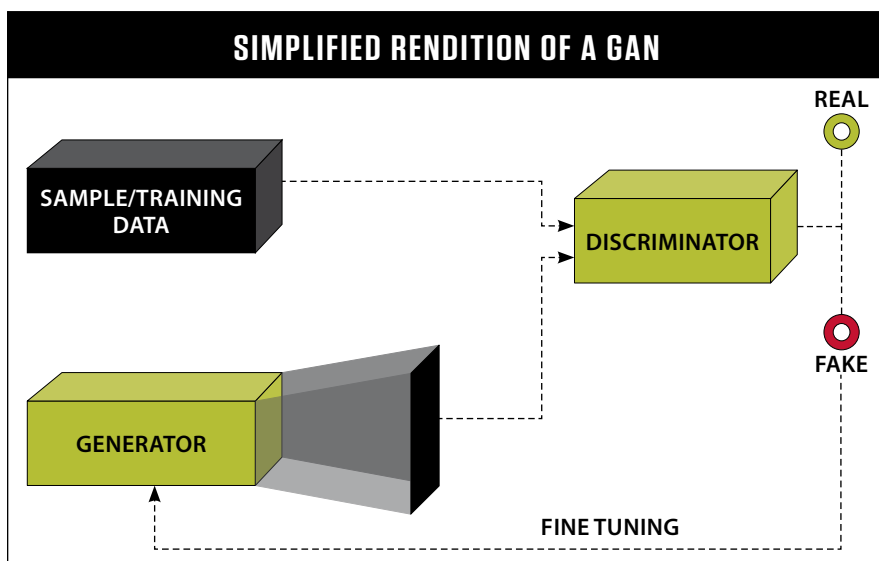


Figure 01

The video was the work of one individual, a user on Reddit who went by the name *deepfakes*.<sup>12</sup> A self-described programmer with an interest in machine learning, *deepfakes* was able to produce the Gadot video using entirely open-source machine learning tools.<sup>13</sup> Working behind the scenes to power his algorithm was Goodfellow's innovation, the GAN.

Then, in June of 2019, the "DeepNude" app launched. The app took pictures of fully clothed women submitted by users and then produced a realistic nude picture of them.<sup>14</sup> While it was eventually pulled offline due to mounting public pressure and negative press coverage, the source code was first copied and immortalized on the Internet.

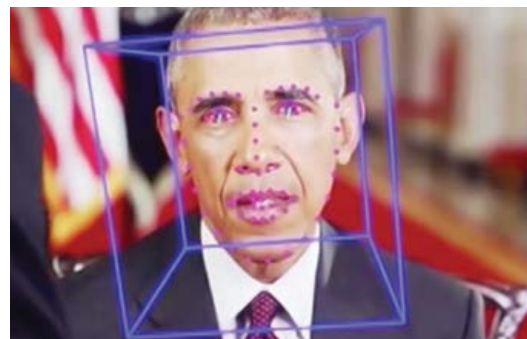
One may rightly wonder how the GPC and twisted fantasies lived out on the internet relate. What is of great significance to U.S. national interests and security is the technology behind how these videos were created. It is of especially great interest to those of us operating predominantly in the IE that these videos were entirely convincing to large audiences. The implication for the future of information warfare ought to be forming more clearly: There exists the technology to produce a video of anyone saying or doing anything that they have never said or done in a place that they have never been.

### The Unique Nature of Synthetic Media

There are those who argue that the concern over synthetic media and AI is overblown. This argument is not without merit. It is true that new technologies have historically been met with disproportionate and unwarranted skepticism. However, there are reasons as to why synthetic



02



03

media ought to be considered separately and demands unique attention.

What makes it so different? The answer lies not in one simple factor but rather in the convergence of multiple ones, all contributing to the perfect environment for disinformation to thrive. These factors are psychological, technical and sociological: The perceived trustworthiness of visual information, the difficulty in falsifying synthetic media and truth decay.

**I. Processing Fluency:** Research has well-established the fact that if people are repeatedly exposed to a statement, it becomes more likely that they will judge it to be true.<sup>15</sup> This has been proven in two distinct situations: 1) When an individual is exposed to a statement numerous times and *recalls* the previous exposure; and 2) When an individual is exposed to a statement numerous times but *does not recall* the previous exposure.<sup>16</sup>

The latter is the more complex situation and offers insight into the power of synthetic media. While the individual does not recall the previous exposure, processing fluency — or the ease with which information moves through the cognitive





Figure 01

Generative Adversarial Networks use two artificial intelligence algorithms — one generates the fake content and the other grades its efforts — teaching the system to be better in order to create more accurate deepfakes.

Deepfakes are fake content (videos, photos or audio) created using a form of AI called deep learning (hence the name deepfake). The AI can learn what a source face looks like and then transpose it onto another target to perform a face swap. Computers can be fed enough data to generate fakes which behave like a real person.

02

Actor Jordan Peele (right) created a deepfake video by inserting his voice and mouth movements over an original video of former President Barack Obama to showcase how technology can be used to make *anyone say anything*. VOA News

03

Software can analyze video content to determine if it is fake but oftentimes the fraudulent content is already viral by the time it's discovered. VOA News

an audience of 1,500 people at a rate of six times faster than the truth.<sup>25</sup> The spread of disinformation will not wait for verification.

The second issue is that detection relies on trust. If Facebook detects a deepfake and labels it as such, it will only be successful if people trust Facebook as an honest actor. If not, it is rather inconsequential. The same goes for a Defense Advanced Research Agency funded initiative, for instance, which ought to demand trust. This is hardly guaranteed.

**III. Truth Decay:** Over the past decade, an unfortunate trend has unfolded in the United States known as truth decay.<sup>26</sup> In a report; authored by Jennifer Kavanagh and Michael D. Rich of the RAND Corporation, in 2018, truth decay was defined by breaking it into four inter-related sub-trends: increasing disagreement over facts, distortion of the line separating opinion from fact, increasing volume and subsequent influence of opinion and personal experiences over facts and decreased institutional trust in formerly respected sources of information.<sup>27</sup>

All of these contribute to an IE where disinformation thrives. Consider that from 2001-2015, the percentage of Americans who believed it is “extremely important” for parents to get their children vaccinated fell 10 percent.<sup>28</sup> This makes little sense given the data surrounding vaccines has only gotten stronger during this very time.<sup>29</sup> Yet the anti-vaccination movement continues to grow. This is the direct result of truth decay. Facts are no longer overwhelmingly agreed upon (e.g. – the efficacy of vaccines); personal experiences carry more weight than robust data (e.g. anecdotal evidence about severe reactions to vaccines) and distrust in traditional media and other formerly respected sources of information have caused people to seek the “truth” elsewhere (e.g. consulting social media influencers instead of the Center for Disease Control).

While there have been previous instances of what looks like truth decay in American history, Kavanagh and Rich found that there is “no evi-

system<sup>17</sup> — is at work. As one is repetitively exposed to a statement, it becomes easier to process. The easier information is to process, the more likely it is that one will trust it.<sup>18</sup> Furthermore, there is evidence that processing fluency has positive effect. In other words, “high fluency [information] is subjectively experienced as positive.”<sup>19</sup> This means that not only will the consumer of the information be more likely to trust it, they will also be more likely to have a positive association with it.

The danger is that visual stimuli typically have high fluency. Our brains are hardwired to trust visual information, and synthetic media makes it impossible for the individual to discern between what is real, what is synthetically altered and what is wholly AI generated. This creates a compounding effect in which humans are naturally inclined to believe the information presented but also lack the ability to verify it. This leads to the next factor: Falsifiability.

**II. Falsifiability:** Synthetic media’s falsifiability — or, more accurately, the lack thereof — separates it once again from previous digital media manipulation tools. Put bluntly, in a 2019 report by the Brookings Institution: “Deepfakes...can be literally perfect: There is an attainable point in which deepfakes can be entirely indistinguishable from authentic content.”<sup>20</sup> This has not been true of past technologies.<sup>21</sup>

One aspect of the falsification problem lies in the main detection approach. Much of the research thus far has looked at developing more sophisticated automated detection systems, which makes sense as humans lack the ability to do so. However, recall that GANs use two competing neural networks, one being a discriminator (or detector). As researchers develop detection methods that work, it counter-intuitively serves as a sort of roadmap for the very developers of the altered media.<sup>22</sup> These developers can effectively incorporate the detection into their very own system, rendering it obsolete.

Beyond this, other issues remain. First, the nature of detection means that it necessarily comes after the fact.<sup>23</sup> Even if one could detect a fake video within 15 minutes, for instance, the rapid spread of information on the Internet means it could potentially reach an audience so wide in such a short period of time that detecting its inauthenticity would be rather ineffective. Researchers at the Massachusetts Institute of Technology have shown that falsities spread faster and deeper online than the truth “in all categories of information.”<sup>24</sup> In fact, they found that falsehoods reached

dence of fundamental disagreements over objective facts” in any of the previous historical case studies.<sup>30</sup> The introduction of synthetic media into an IE suffering from such vulnerabilities is concerning. This is not unique to America, either.<sup>31</sup> As this trend continues to develop globally, disinformation targeting the United States will become equally — if not more — effective abroad than it already is domestically.

These three factors — fluency, falsifiability and truth decay — contribute to the seriousness of the synthetic media threat. It produces a nearly impossible situation for information consumers: Information is presented in a form that one is inherently more likely to trust, yet is also impossible to verify and the institutions that people have historically relied upon to conduct quality-assurance and quality-control of information are no longer widely trusted. Given these conditions, how does one seek truth?

## GREAT POWER COMPETITION

### *Russian Sponsored, AI Empowered Disinformation*

There are two distinct threats from the use of synthetic media for disinformation purposes. The first would be individual users spreading false information with the help of democratized and decentralized AI tools. While this is important and will present unique national security problems, this article is concerned with the second use of synthetic media: state sponsored disinformation. Particularly troubling will be Russia’s use of said technology as Moscow has shown no signs of slowing its information warfare campaign against the U.S.

To fully appreciate this threat, a brief look at Russian “active measures” is in order. Active measures, for the purpose of this article, can be defined as planned covert or overt uses of disinformation by a state actor intended to harm an adversary. This will be followed by an analysis of the impact that synthetic media will have in the GPC and recommendations for combatting the threat.

### *A Brief Look at Russian Active Measures*

The Kremlin’s information warfare strategy has a long history, tracing back to the 1917 revolution and Operation Trust, which created the first known unit dedicated to disinformation.<sup>32</sup> However, its more modern origins begin in 1942 with the introduction of *spetspropaganda* (special propaganda) theory at the Military Institute of Foreign Languages.<sup>33</sup>

Described by one former KGB Cold Warrior as the “heart and soul of Soviet intelligence,”<sup>34</sup> another defector, Yuri Brezmenov, provided further insight: “Only about 15 percent of time, money, and manpower is spent on espionage as such. The other 85 percent is what we call ideological subversion or active measures.”<sup>35</sup> He continued, revealing the intent of such measures: “What this basically means is to change the perception of reality for every American to such an extent that despite the abundance of information, no one is able to come to sensible conclusions...”<sup>36</sup>

Examples of these efforts abound. Some operations proved significant but were rather narrow in scope, such as aligning the votes of two West German legislators with Soviet interests regarding the removal of West German Chancellor Willy Brandt in 1972.<sup>37</sup> Others were more nefarious, closer to the description that Brezmenov provided, including the effort to convince Americans that the Central Intelligence Agency assassinated President Kennedy.<sup>38</sup>

One of the greatest active measures taken during this time began in the early 1980s and has consequences still today: Operation INFEKTION. The Soviets successfully spread the false narrative that the HIV/AIDS health crisis was a product of the U.S. government, particularly scientists and the military.<sup>39</sup> Soviet propaganda also claimed that the disease was being used as an ethnic weapon targeting black Americans.<sup>40</sup> In the United States, public opinion polling provides insight into the long-term efficacy of the operation. In a 2005 study, 53 percent of African Americans polled believed that “there is a cure for AIDS, but it is being



01



02

01 Soviet *spetspropoganda* spreading the false narrative that the HIV/AIDS health crisis was a product of the U.S. government being used as a weapon to target black Americans and homosexuals. CIA IMAGE

02 Caption above cartoon states: The AIDS virus, a terrible disease for which up to now no known cure has been found, was, in the opinion of some Western researchers, created in the laboratories of the Pentagon. Words on the flag on the beaker state: Virus AIDS. Caption below reads: Pentagon (AIDS) specialists. PRAVDA DAILY PAPER, OCTOBER 31, 1986

03 In 2020, Tulsa Police Major Travis Yates (right) said his comments were misrepresented in an on-air interview with RT (Russia Today), and it wasn't until after the interview that he learned it was a Russian-backed news operation. VOA NEWS

withheld from the poor” and 27 percent agreed that “AIDS was produced in a government laboratory.”<sup>41</sup> More shockingly, 16 percent agreed that the government created AIDS to control the black population and 15 percent believed that it is a form of genocide against African Americans.<sup>42</sup> One cannot attribute these results solely to Operation INFEKTION. As is typical for active measures, the operation exploited *existing* social tensions but did not create them. Nevertheless, it is difficult to imagine these staggering numbers without INFEKTION’s influence.

With the fall of the Soviet Union came the reorganization of its military education system, but that did not mark the end of active measures. *Spetspropaganda* did not fade into oblivion but was rather re-incorporated more broadly, becoming arguably even more important to Russian strategy. Today, classes on information warfare are taught not only to the Russian military but are also included in diplomatic training, as well as in sociology, philosophy, and political science departments across numerous universities.<sup>43</sup>

The experience Russia has built executing active measures is evident in its effective annexation of Crimea in 2014. Every tool available to the Kremlin was used in this effort, to include federal television and radio channels, newspapers, and, of course, online outlets.<sup>44</sup> It was a methodically executed operation supported by actors across numerous institutions in Russia, from diplomats to academics.<sup>45</sup> Its success is evident in the fact that Crimea, the victim of the aggression, simply did not resist. “This happened,” writes Jolanta Darczewska for the Warsaw-based think tank, the Centre for Eastern Studies, “because Russian-speaking citizens of Ukraine...had undergone necessary psychological and informational treatment.”<sup>46</sup>

Then came the 2016 U.S. Presidential Election. In April of 2014, Russian influence operations were already underway.<sup>47</sup> One of the organizations that emerged from this effort was the Internet Research Agency operating out of St. Petersburg.<sup>48</sup> The IRA has been described as a troll farm, although this is an easily dismissed label that does a disservice to the agency’s scale and reach. More accurately, the IRA is a “Kremlin-backed enterprise staffed with hundreds of people whose main job is to sow disinformation on the Internet.”<sup>49</sup> The agency used social media influence operations to exploit social tensions in the U.S., particularly around identity-based issues such as race, to shape both voter perceptions and participation

rates.<sup>50</sup> Some measures of performance are particularly impressive. For example, one IRA-controlled Facebook group, “Blacktivist,” gained an audience of more than 360,000 people, amounting to more than the official Black Lives Matter page.<sup>51</sup>

Quantifying the impact of this election interference campaign has proven difficult. However, it is certainly clear that Russia has every intention to continue its longstanding campaign of active measures aimed at destabilizing the United States and degrading its global influence.

### Great Power Competition in a Post-Truth World

While the American experience has been largely defined by transnational terrorism in the first decades of the 21st Century, threats posed by state actors — primarily China and Russia, but including Iran and North Korea, as well — have made their way to the top of Washington’s priority list.<sup>52</sup> In the *2018 National Defense Strategy*, the first since 2008, this shift was clear. Then Defense Secretary James Mattis said the following in a speech introducing the updated strategy: “We will continue to prosecute the campaign against terrorists that we are engaged in today, but great power competition, not terrorism, is now the primary focus of U.S. national security.”<sup>53</sup>

When discussing this shift, a false dichotomy is often invoked: either conventional war among the great powers is the main strategic threat to the U.S. or non-state actors and conflict below the threshold of war is. This is a fundamental misunderstanding of the GPC, as well as where it is heading. These threats are not mutually exclusive. While America’s near-peers are the greatest strategic threat to the United States, it is their use of





irregular tactics and techniques that fall below the threshold at which the U.S. would respond with conventional forces that is the danger.

There is recognition of this within the Department of Defense, evident in the 2020 unclassified summary of the Irregular Warfare Annex to the 2018 *National Defense Strategy*. Remaining proactive in the GPC and emphasizing operations within the information environment rank among the five core themes of the IW annex; the former recognizes that the GPC involves conflict of an ongoing nature, not limited in scope to merely conventional war, and the latter stresses the important role of information operations.

Ezra Cohen, the former Acting Under Secretary of Defense for Intelligence and Security, stated in a recent symposium that the U.S. must “accept that influence is an integral aspect of modern warfare, not just a niche capability.”<sup>55</sup> By focusing on all-out war, he argued, we risk “missing the contest already underway” in the IE where our “adversaries have weaponized disinformation and propaganda to their advantage.”<sup>56</sup>

This, not conventional war, presents the greatest challenge in the GPC. One can measure the seriousness of a threat by assessing an adversary’s capability and intent to execute. Certainly, Russia has both the capability and intent to conduct disinformation campaigns against the U.S. It is highly unlikely that Russia would risk force-on-force war, but information warfare provides an asymmetric option short of open conflict.

It appears that obtaining regional influence over former Soviet Union states is what drives Russian activity. In pursuit of this, Moscow will continue to execute active measures intended to destabilize the United States domestically, as well as damage its reputation and credibility globally. If successful, these measures 1) make it difficult to form the national will necessary to maintain America’s hegemonic status and 2) seriously degrade America’s ability to compete in the region of former Soviet Union countries, among elsewhere. These measures will also continue to undermine the North Atlantic alliance, a critical aspect of preventing Russian regional dominance.

Synthetic media makes executing these active measures easier by orders of magnitude. A key aspect to Russian information warfare is

**A KEY ASPECT TO RUSSIAN INFORMATION WARFARE IS TO PRODUCE SUCH A HIGH VOLUME OF DISINFORMATION THAT PEOPLE EITHER BECOME DISINTERESTED IN THE TRUTH OR DISTRUST ALL SOURCES OF INFORMATION.**

01

Deceptive Russian social media ads from fake organizations feature content designed to stoke fear on contentious issues and disrupt relationships between legislators, law enforcement and the public in order to increase the divide between the groups.



to produce such a high volume of disinformation that people either become disinterested in the truth or distrust all sources of information altogether. With synthetic media, this strategy becomes even more effective. It may take only a few deepfake videos to dissuade people from seeking the truth. As deepfakes become more common, it will subsequently become harder for people to trust *any* information. The result of this means the potential dismissal of all U.S. government media, for instance, which would render the important influence capability referenced by Under Secretary Cohen as nearly unattainable.

This type of IE also offers Moscow something of great value: the liar’s dividend. When reality and forgery are indistinguishable, those who spread false information and act in bad faith benefit the most. Since the technology exists to create perfectly falsified media, then seeing does not equal believing and it stands to reason that all media could potentially be fake; if all media could *potentially* be fake, then there is absolutely nothing that Russia could not reasonably deny. It is a vicious epistemological crisis. This would embolden a Russia that has made aggressive moves over the past decade in pursuit of greater regional influence. Moscow’s bold denials of well-documented operations in Crimea, for example, is an indication of how Russia will leverage this new dynamic in pursuit of their goals.

While the term post-truth has been used all-too liberally in the past, it is perhaps closer to reality than ever before. There is no conceivable situation in which this benefits the United States. Truth decay is one of the factors that contribute to the effectiveness of deepfakes, but it also further

accelerates because of them. This consequence is perhaps most damaging of all: the further degradation of the truth. These conditions make America more susceptible to domestic instability and less capable of effectively exerting influence globally. Of course, this meets the very intent of Russian active measures. *Change the perception of reality to such an extent that despite the abundance of information no one is able to come to sensible conclusions.*

## RECOMMENDATIONS


The following are recommended actions that will assist America, the Army, and Psychological Operations to meet this challenge head on:

1. Most importantly, we need a robust and apolitical public service campaign that aims to educate the American people on Russian and other state sponsored disinformation campaigns, as well as on artificial-generated media.<sup>57</sup> This will not come from PSYOP, but ought to come from a trusted institution such as the military. The best defense against disinformation is preventive in nature.
2. The recently formed Army Artificial Intelligence Task Force has four focus areas and should add a fifth: information operations. Ensuring a PSYOP presence within the Task Force is paramount.
3. A “train with industry” program should be established that place career-oriented PSYOP Officers in private-industry AI companies that are at the forefront of developing synthetic media and deepfake detection. Knowledge of how deepfake detection works will prove valuable in

the future when countering synthetically generated propaganda.

4. A “program of record” ought to be established that brings synthetic media capabilities to the regiment.

5. Increase the aggressiveness of IO aimed at undermining Russian credibility and influence by lowering approval authorities for PSYOP operations. We must match the speed and volume with which Russian actors disseminate disinformation must be matched.

Adopting these recommendations would better prepare the United States for the coming threat of synthetic media and deepfake disinformation. Failing to do so could have potentially enormous consequences. 

## ABOUT THE AUTHOR

**CPT Benjamin J. Levine** is a Psychological Operations Officer who served as a Detachment Commander in A Co., 8th Psychological Operations Battalion (Airborne) before serving in his current role as Executive Officer for D Co., 3rd POB(A).

**NOTES** 01. James Vincent, “Putin Says The Nation that Leads in AI ‘Will Be the Ruler of the World,’” *The Verge*, September 4, 2020, <https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world>. 02. Clint Watts, “Russia’s Active Measures Architecture: Task and Purpose,” *Alliance For Securing Democracy*, June 11, 2018, <https://securingdemocracy.gmfus.org/russias-active-measures-architecture-task-and-purpose/>. 03. Ibid. 04. Throughout the article, synthetic media and deepfakes will be used interchangeably, although they differ slightly. Synthetic media is any media that is partially or wholly generated using artificial intelligence. Deepfakes is a subset of this, being any synthetic media that is used for dis- or misinformation purposes. However, since this article is only concerned with synthetic media used for disinformation purposes the reader should be aware that when it is referenced it is implying the deepfakes subset (for instance, synthetic media used in the film industry would not be implicated). 05. Martin Giles, “The GANfather: The man who’s given machines the gift of imagination,” *MIT Technology Review*, February 21, 2018, <https://www.technologyreview.com/2018/02/21/145289/the-ganfather-the-man-whos-given-machines-the-gift-of-imagination/>. 06. Ibid. 07. Ibid. 08. Ibid. 09. Geeksforgeeks.org, “Generative Adversarial Network (GAN),” January 15, 2019, <https://www.geeksforgeeks.org/generative-adversarial-network-gan/>. 10. Giles, “The GANfather.” 11. Samantha Cole, “AI-Assisted Fake Porn is Here and We’re All Fucked,” *Vice Magazine*, December 11, 2017, <https://www.vice.com/en/article/gdydym/gal-gadot-fake-ai-porn>. 12. Ibid. 13. Ibid. 14. Samantha Cole, “This Horrifying App Undresses a Photo of Any Woman With a Single Click,” *Vice Magazine*, June 26, 2019, <https://www.vice.com/en/article/kzm59x/deepnude-app-creates-fake-nudes-of-any-woman>. 15. Rolf Reber and Christian Unkelbach, “The Epistemic Status of Processing Fluency as Source for Judgments of Truth,” *Review of Philosophy and Psychology* 1, no. 4 (2010): 563–81, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3339024/>. 16. Ibid. 17. Rolf Reber, “Processing Fluency, Aesthetic Pleasure, and Culturally Shared Taste,” *Oxford Scholarship Online*, <https://oxford.universitypressscholarship.com/view/10.1093/acprof:oso/9780199732142.001.0001/acprof-9780199732142-chapter-009>. 18. Ibid. 19. Rolf Reber, Norbert Schwarz, and Piotr Winkielman, “Processing Fluency and Aesthetic Pleasure: Is Beauty in the Perceiver’s Processing Experience?” *Personality and Social Psychology Review, Inc* 8, no. 4 (2004): 365–366, [https://dornsife.usc.edu/assets/sites/780/docs/04\\_psrp\\_reber\\_et\\_al\\_beauty.pdf](https://dornsife.usc.edu/assets/sites/780/docs/04_psrp_reber_et_al_beauty.pdf). 20. Alex Engler, “Fighting Deepfakes When Detection Fails,” *Brookings Institution*, November 14, 2019, <https://www.brookings.edu/research/fighting-deepfakes-when-detection-fails/>. 21. Chris Meserole and Alina Polyakova, “Disinformation Wars,” *Foreign Policy*, May 25, 2018, <https://foreignpolicy.com/2018/05/25/disinformation-wars/>. 22. Ibid. 23. There is growing research into what is known as “digital watermarking,” which would provide increased security against media manipulation, but this would not be a comprehensive solution to detecting wholly-AI generated synthetic media. 24. Maggie Fox, “Fake News: Lies spread faster on social media than truth does,” *NBC News*, March 9, 2018, <https://www.nbcnews.com/health/health-news/fake-news-lies-spread-faster-social-media-truth-does-n854896>. 25. Ibid. 26. Kavanagh, Jennifer and Michael D. Rich, “Truth Decay: A Threat to Policymaking and Democracy,” *Rand.org*, 2018, [https://www.rand.org/pubs/research\\_briefs/RB10002.html](https://www.rand.org/pubs/research_briefs/RB10002.html). 27. Ibid. 28. Ibid. 29. Unicef.org, “Immunization,” July 9, 2019, <https://data.unicef.org/topic/child-health/immunization/>. 30. Kavanagh and Rich, “Truth Decay.” 31. Indranil Ghosh, “The Global Trust Crisis,” *Foreign Policy*, January 22, 2020, <https://foreignpolicy.com/2020/01/22/davos-world-leader-trust-institutions-populism-protest/>. 32. Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020), 18. 33. Jolanta Darczewska, “The Anatomy of Russian Information Warfare: The Crimea Operation, A Case Study,” *Point of View*, no. 42 (May 2014): 9, [https://www.osw.waw.pl/sites/default/files/the\\_anatomy\\_of\\_russian\\_information\\_warfare.pdf](https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf). 34. Calder Walton, “Active measures: a history of Russian interference in US elections,” *Prospect Magazine*, December 23, 2016, <https://www.prospectmagazine.co.uk/science-and-technology/active-measures-a-history-of-russian-interference-in-us-elections>. 35. Sirena Bergman, “This ex-KGB agent’s account of how to destabilise a nation is eerily relevant,” *Indy100*, November 27, 2019, <https://www.indy100.com/news/kgb-russia-interference-usa-uk-putin-9218891>. 36. Ibid. 37. Richard Tilley, “The Kremlin’s Return to Active Measures,” *review of Active Measures: The Secret History of Disinformation and Political Warfare*, by Thomas Rid, <https://www.lawfareblog.com/2020/10/20/the-kremlins-return-to-active-measures/>. 38. Fred Litwin, “The Soviets and the JFK Conspiracy Theorists,” *Quillette*, September 27, 2018, <https://quillette.com/2018/09/27/the-soviet-and-the-jfk-conspiracy-theorists/>. 39. Thomas Boghardt, “Operation INFEKTION,” *Studies in Intelligence* 53, no. 4 (December 2009): 4, <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no4/pdf/U-%20Boghardt-AIDS-Made%20in%20the%20USA-17Dec.pdf>. 40. Ibid. 41. *Rand.org*, “Study by RAND and Oregon State University Finds Conspiracy Beliefs Among African Americans Deter Condom Use,” <https://www.rand.org/news/press/2005/01/25.html>. 42. Ibid. 43. Darczewska, “The Anatomy of Russian Information Warfare,” 10. 44. Ibid. 45. Ibid. 46. Ibid. 47. Abigail Abrams, “Here’s What We Know So Far About Russia’s 2016 Meddling,” *Time*, April 18, 2019, <https://time.com/5565991/russia-influence-2016-election/>. 48. Ibid. 49. Krishnadev Calamur, “What Is the Internet Research Agency?” *The Atlantic*, February 16, 2018, <https://www.theatlantic.com/international/archive/2018/02/russia-troll-farm/553616/>. 50. Ibid. 51. Donnie O’Sullivan and Dylan Byers, “Exclusive: Fake black activist accounts linked to Russian government,” *September 28, 2017*, <https://money.cnn.com/2017/09/28/media/blackactivist-russia-facebook-twitter/index.html>. 52. Ronald O’Rourke, “Renewed Great Power Competition: Implications for Defense—Issues for Congress,” *Congressional Research Service*, October 29, 2020, <https://crsreports.congress.gov/product/pdf/R/R43838.1>. 53. Idrees Ali, “U.S. Military Puts ‘great Power Competition’ at Heart of Strategy; Mattis,” *Reuters*, January 19, 2018, <https://www.reuters.com/article/us-usa-military-china-russia-idUSKBN181TR>. 54. Department of Defense, “Irregular Warfare Annex to the National Defense Strategy - Summary,” 2020, <https://media.defense.gov/2020/Oct/02/2002510472/-1/-1/0/Irregular-Warfare-Annex-to-the-National-Defense-Strategy-Summary.PDF>. 55. David Vergun, “Great Power Competition Can Involve Conflict Below Threshold of War,” *DOD News*, October 2, 2020, <https://www.defense.gov/Explore/News/Article/Article/2364137/great-power-competition-can-involve-conflict-below-threshold-of-war/>. 56. Ibid. 57. Studies have shown that revealing the source of propaganda can be effective; Facebook users are less likely to spread Russian propaganda when they know the source.



# COMPREHENSIVE DEFENSE: A Whole-of-Society Approach via Irregular Forces

Adding to global deterrence and defense against aggressors  
without breaking the bank.

BY LIEUTENANT GENERAL (RETIRED) ERIC WENDT

We live in a time bedeviled by hostile Great Powers, rogue states and terrorist networks. To cope with these aggressors in a financially sustainable way, the United States and its friends throughout the free world must better incorporate irregular forces using a host country financed, whole-of-society comprehensive defense approach.

Historically, many countries have successfully developed irregular force/whole of society CD capabilities. These forces were taught fundamental defensive tactics and provided with basic equipment needed to defend their towns, cities, ports, mountain passes and more. Just a few examples showcasing irregular force CD include the militias of the city-states of ancient Greece. In the 1930s, the Swiss prepared significant numbers of irregulars to effectively deter Nazi

aggression. And in 1940, irregular/civilian maritime participation at Dunkirk helped evacuate more than 300,000 imperiled Soldiers stranded and surrounded. Today, various levels of irregular force CD is growing in Sweden, Finland, Estonia, Latvia, Lithuania and a small number of other countries.

Globally, all countries threatened by, or of strategic value to, an aggressor should prepare all volunteer, irregular force CD. Precient leaders of such countries can permanently specialize a portion of their regular land, sea and air forces as irregular force trainers. Each country can be divided into districts (*see figure 01*), and three-day long fully voluntary training segments (with a small amount of host-country provided pay for volunteers) can be completed throughout the course of a year in each individual town, city, port, etc. The training teams stay with their

01  
Members of the Lithuanian National Defence Volunteer Forces and U.S. Army Special Forces conduct a mission planning exercise.  
U.S. ARMY PHOTO BY SGT. KAREN SAMPSON

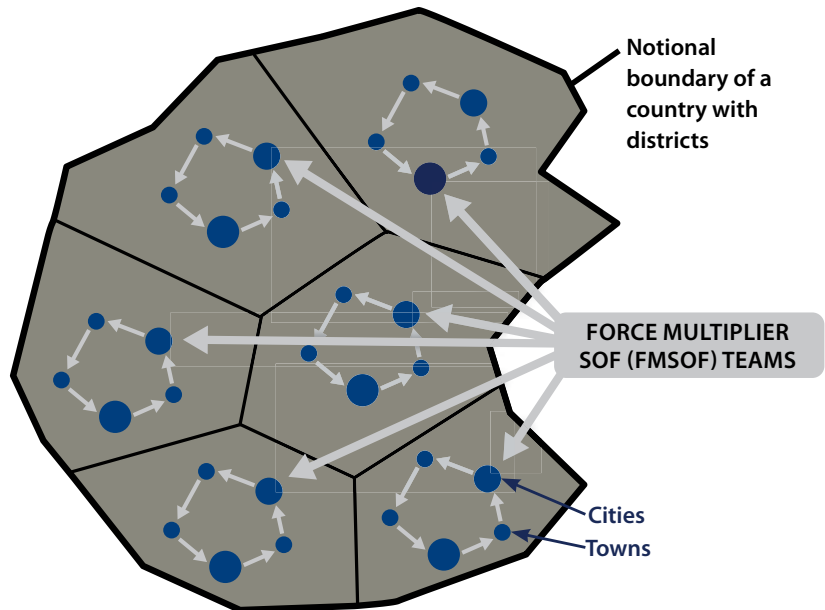
## FIGURE 01: RECOMMENDED NATIONAL COMPREHENSIVE DEFENSE EXERCISE

Countries can use Force Multiplier SOF as mobile training teams to rotate through their country each year to conduct three-day comprehensive defense exercises with volunteers from the local population.

Volunteers should receive a small amount of host-country provided pay for participation in the exercise.

### Benefits Include:

1. Increase deterrence and defense against external threats.
2. Create a “neighborhood watch” network capability that improves domestic counter-terrorism reporting to other government agencies who investigate issues reported.
3. Develop networks which can effectively support humanitarian-relief efforts inside the country.
4. All funding used for pay, equipment, exercises and other items for comprehensive defense “counts” towards the 2% of GDP goal for NATO Allies.



*Over the course of a year every town/city within each district conducts a three-day comprehensive defense exercise.*



Recommend using the NSHQ Comprehensive Defense Handbook

assigned CD districts in future years to nurture strong, enduring personal relationships with locals.

CD forces consist of significant numbers of men and women of all adult ages, from able bodied to handicapped. These patriotic volunteers will prepare solely to defend their hometowns and local areas. They train in myriad tasks such as coastal or mountain pass watchers; as observers of aircraft overflights; and as small light infantry cells, units and more. They do not threaten others outside their borders; however, they pose a daunting challenge to potential aggressors.

In addition to regular small arms weaponry used throughout the CD forces, specially vetted elements of these CD units may also be able to utilize anti-armor, anti-air weapons, and may learn to operate armed drones and other weaponry.

The U.S. may choose to assist using skilled U.S. trainers if

## GLOBALLY, ALL COUNTRIES THREATENED BY, OR OF STRATEGIC VALUE TO AN AGGRESSOR SHOULD PREPARE ALL VOLUNTEER, IRREGULAR FORCE COMPREHENSIVE DEFENSE.

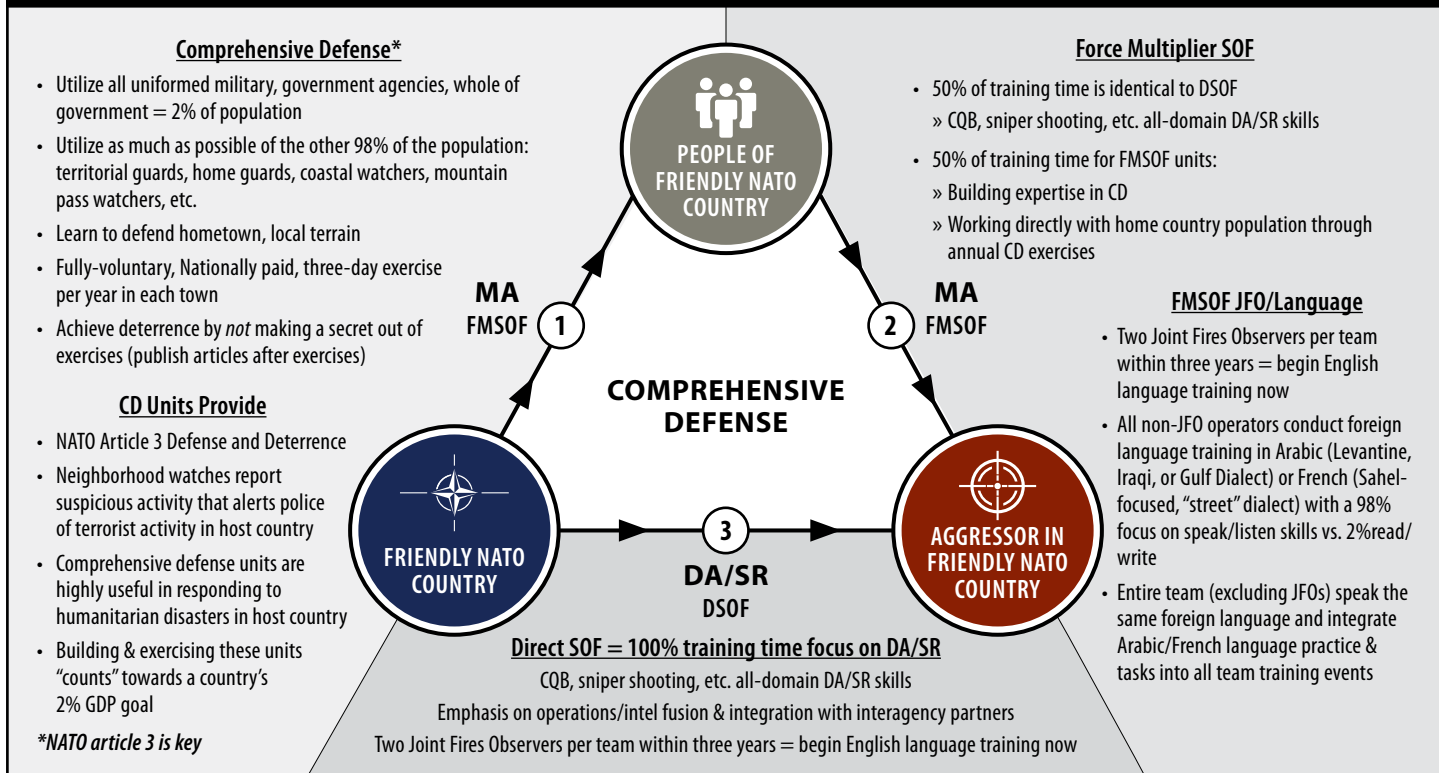
requested and invited by a host country. Ideally U.S. land, sea and air trainers should have language and cultural skills, and (like the Green Berets of the numbered Special Forces Groups) already be skilled training irregular forces. U.S. training of CD units can be either direct (directly training the foreign locals in CD units) or indirect, “training the trainers” of the host country’s services.

The creation of irregular CD forces may encounter resistance from some in their countries’ defense establishment. Some defense and military leaders with calcified mindsets may be reluctant to work

in what is to them the unfamiliar world of irregular forces. And some weapons companies with significant lobbying power (and significant ties to some political leaders) may resist an irregular approach that emphasizes the inexpensive armaments utilized by these CD units, reducing their potential revenues.

Once formed and trained, irregular CD units should be brought into conventional military wargames, so that senior military leaders can begin to understand how to better defend their countries using the mass the significant numbers of irregular forces and effective capabilities CD provides.

**FIGURE 02: SOF ROLES IN SPECIAL RECONNAISSANCE, DIRECT ACTION AND MILITARY ASSISTANCE**



## The North Atlantic Treaty — Article 3 —

In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack.

Additionally, some may be concerned that a government may misuse CD units to oppress their populations. But it is more likely that volunteer CD units trained to defend their homes will prove a strong guarantee of freedom against any overbearing central government regime that might arise.


CD units can also provide humanitarian assistance in the wake of natural disasters within their own

country, providing trucks, doctors, security and many other capabilities.

Notably, among NATO members, the money spent on CD units "counts" toward meeting goals like the Alliance's 2 percent of Gross Domestic Product defense spending, while simultaneously bolstering NATO's Article 3 which enjoins all members to build resilient defenses.

Some good news, in 2020, using significant input from Nordic, Baltic and other countries, the NATO Special Operations Headquarters developed an easy-to-understand CD handbook and a week-long course covering easily implemented CD techniques. The course is open to NATO members and partner countries. Military or other agency personnel of all these countries may attend. Friends outside NATO, from anywhere on the globe, may also request attendance.

Uniformed military forces must evolve to better utilize nanotechnologies, cyber, space, lasers, armed and unarmed drones, unmanned

land, sea and air vehicles, hypersonic munitions, quantum computing, artificial intelligence, robotics, and more. But these tools must also be better balanced with irregular CD forces to provide effective deterrence and defense at a cost that can be sustained. Irregular CD units will greatly enhance countries' ability to defend themselves ... at their own expense. Now is the time, before aggressors' strike, to implement irregular force CD to develop proactive, effective "Home Alone" deterrence and defense. 

## ABOUT THE AUTHOR

**LTG (R) Eric P. Wendt** served for over 34 years as an active duty US Army commissioned officer, including over four years in the light infantry followed by 30 years as a Green Beret. He served throughout the globe conducting peacetime training and combat operations, retiring in 2021 as the Commander of the NATO Special Operations Headquarters.



# APPLYING GENERAL ADAPTATION SYNDROME FOR OPTIMIZED PHYSICAL PERFORMANCE

| BY DR. STEPHEN MANNINO | Human Performance and Wellness Program Coordinator

Physical preparedness is a critical component of being a successful special operator. An ARSOF Soldier must not only be physically fit, but also durable and available to complete his mission.

The goal of the Human Development Directorate Physiological Performance Program (formerly known as THOR3) is to help the ARSOF Soldiers reach their physical potential by enhancing combat performance (fitness), improving operational readiness (availability) and increasing operational longevity (durability). These goals are achieved through an interdisciplinary approach utilizing

sports medicine, performance nutrition, and tactical strength and conditioning. While all three components work synergistically to physically prepare the ARSOF Soldier, the focus of this article is the common thread between those three disciplines. While injury prevention/rehabilitation, proper nutrition and a scientifically designed strength and conditioning program are the foundation of improving physical preparedness, a Soldier's full physical potential can never be realized without proper recovery from training.

## General Adaptation Syndrome

It has been said that *"training does not improve performance, recovering from training improves performance."* This statement was validated by Hans Selye, a medical doctor and researcher who developed the theory of General Adap-

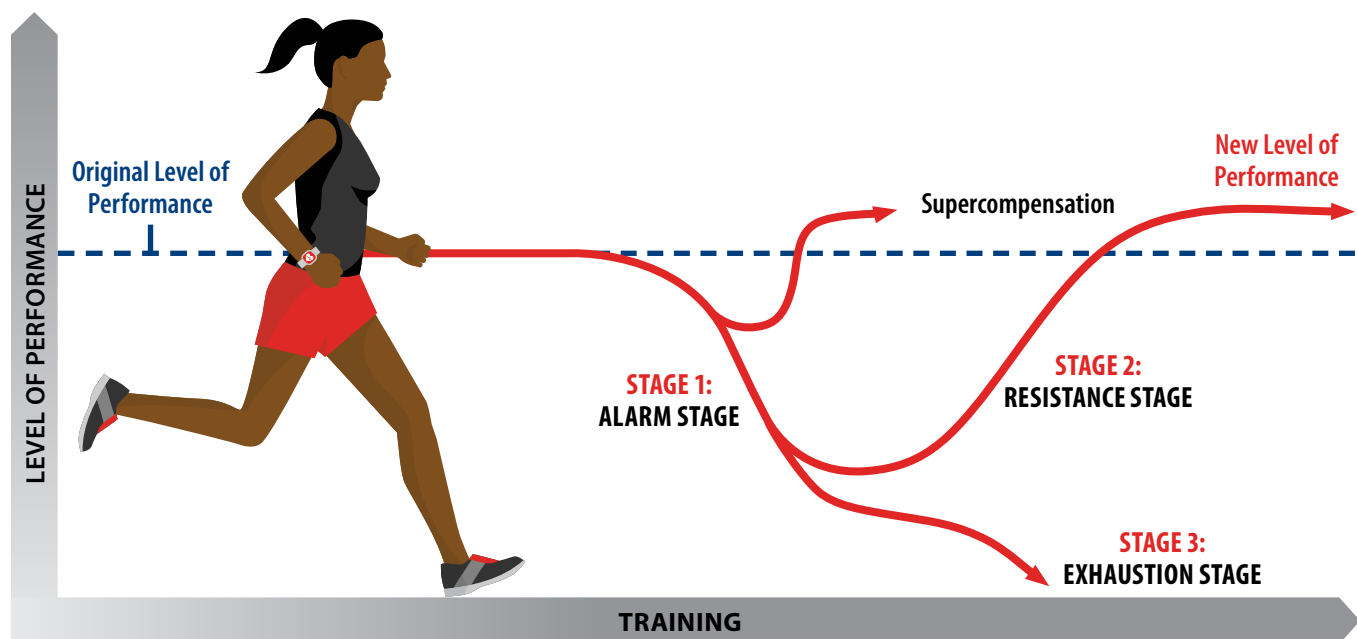
tation Syndrome. GAS is the three-stage process that describes the body's physiological response to stress. In the case of improving physical preparedness, "stress" is the physical training in which a Soldier may participate.

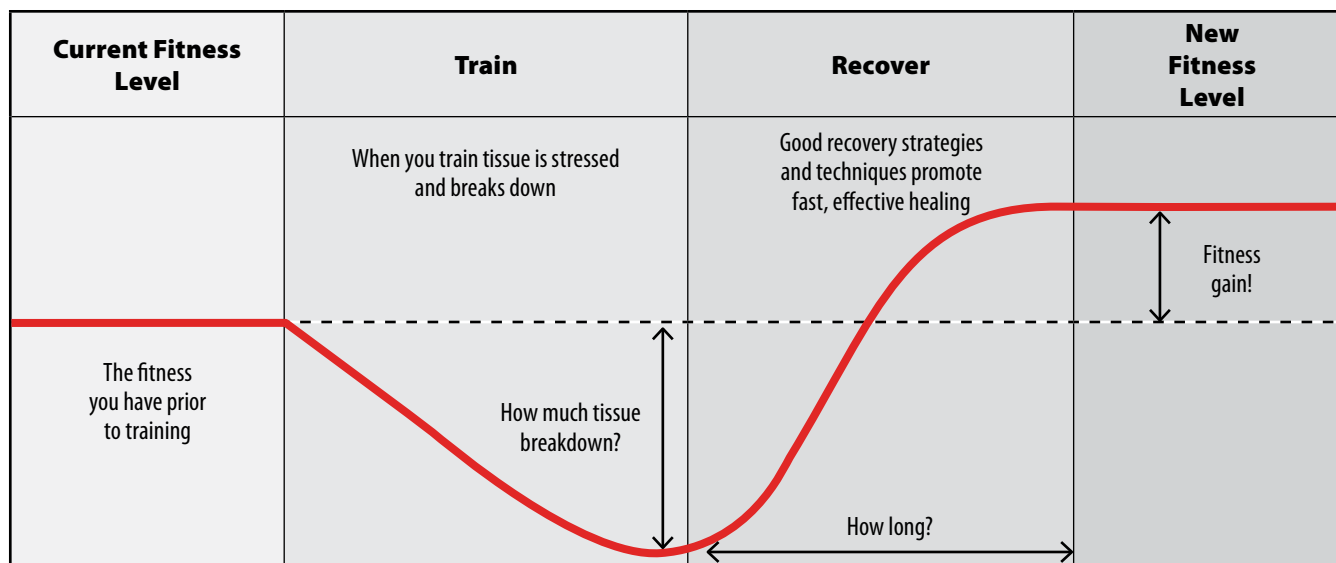
### Stage 1: Alarm Stage

The first stage is the "alarm stage" in which the initial response to stress is first recognized. This "fight or flight response" stimulates the sympathetic nervous system in which the body produces a hormonal responses elevating heart rate, increasing adrenaline and cortisol levels and raising blood pressure. If the stress is removed, the body typically returns to its normal homeostatic state.

### Stage 2: Resistance Stage

The second stage is the "resistance stage." If stress recurs or continues for a period of time, the body will make adjustments. The type of train-





ing (or stress) that is performed determines the type of protein synthesized during recovery, thus the need for specificity of training in order to make performance improvements.

### Stage 3: Exhaustion Stage

If recovery is not sufficiently applied, the third stage, the “exhaustion stage” occurs. If long-term stress is not removed, the body becomes fatigued and overuse injuries begin to surface.

### Recovery as part of a Training

When following a training plan, how the body reacts to and recovers from, stress should be considered. The following guide can assist in making correct choices when it comes to training:


- 1. Training should be reflective of the desired adaptation.** Targeting the proper energy systems and movement patterns will allow for a better transfer from training to the real world.
- 2. Train according to the current level of physiological functioning.** Training age and current fitness levels will determine how the body will adapt to and recover from the stress of training.
- 3. Apply enough training that allows you to recover from fatigue in a reasonable amount of time.** Train-

ing with more volume or intensity than can be recovered from in a moderate timeframe will lead to performance decrements.

- 4. Always factor recovery into a training plan.** As stated previously, training does not improve performance, recovering from training improves performance. Be sure to include active and passive recovery days into a training plan. When appropriate, utilize modalities to assist with recovery. The Normatec Recovery System and GameReady devices are good options, as is massage, and hot and cold-water therapy. Also, mindfulness training or yoga can help stimulate a parasympathetic nervous system response, facilitating recovery.
- 5. Proper recovery after training will lead to supercompensation.** Supercompensation is the point at which you will see performance improvements.
- 6. Stress is stress.** The body cannot discern between the stress placed upon during training, or various life stressors. Everyday stressors, such as work, family, financial obligations compound that of training stress and if not mitigated can be a detriment to the ability to perform in the moment. Minimizing the stress of everyday life as much as possible, help with the optimization of the training process.

**7. Reversibility.** If you don’t use it, you lose it. If the recovery period is too long, performance will begin to decline.

Applying the concept of General Adaptation Syndrome to a training plan will assist in determining how to apply the appropriate amount of stress at the appropriate time. By doing so, the body is able to recover from, and adapt to, the stress of training, leading to improved performance while mitigating the risk of overtraining/under recovered injuries.

To find out more about the practical application of techniques to help optimize training and recovery, contact your unit Human Performance and Wellness coordinator. 

### ABOUT THE AUTHOR

**Dr. Stephen Mannino** is the Human Performance and Wellness Program Coordinator at the U.S. Army JFK Special Warfare Center and School. He has worked as a strength and conditioning coach at several Division I collegiate programs, as well as with professional sports organizations. He holds numerous professional certifications, has earned bachelor’s and master’s degrees in health and physical education from The Citadel, and a doctorate in kinesiology from the University of North Carolina-Greensboro.

# PREDATORY STATES: OPERATION CONDOR AND COVERT WAR IN LATIN AMERICA

It has been 16 years since J. Patrice McSherry published her provocative account of the U.S. role in Operation Condor: an extrajudicial and institutionalized use of political violence and repression in Latin America during the 1970s and '80s. Yet despite the book's age, it remains a relevant and thought provoking assessment of the potential unethical employment of the state's security resources to address asymmetric problem sets.

*Predatory States: Operation Condor and Covert War in Latin America* includes painstaking analysis of CIA, Defense, and State Department support to the transnational and parastatal security structure known as Condor. Its goal was to defeat leftist ideology and progress, while preserving domestic power structures. Human rights abuses saturated the institution. McSherry presents Condor through a counterinsurgency lens. Condor transformed the relationship between the state and society and extended repressive state power to a deniable security apparatus. For Condor's creators, conflict was no longer limited to traditional warfare domains. Instead, in their estimation, preserving national interest relied upon all available means to control 'internal enemies,' inhibit progressive ideas of social welfare and justice and prevent revolutionary threats.

One of *Predatory States'* strengths is McSherry's historical perspective, which links Condor to earlier U.S. policies outside of Latin America. The book contends Condor received funding, training and operational support from the United States in a model transplanted from a predecessor program in Europe. McSherry's wide aperture links Condor to how the Allied forces shifted to fighting a new "ideological war" via parallel 'stay-behind armies' at the cessation of hostilities in World War II. This shadowy structure continued into the Cold War period. Condor intended to preserve status quo power relations throughout Latin America, protect the oligarchy while "shifting state power...appeared to be within the grasp of previously marginalized social sectors."


Another strength is McSherry's evidentiary base. At the structural level, government reports and first-hand accounts aptly demonstrate Condor was a flourishing transnational institution from the South American Cone to Central America. State-level analysis focuses on operational characteristics of key intelligence organizations that thrived in the parallel state

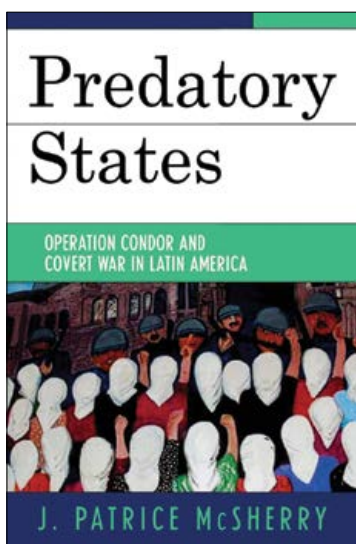
structure, ensuring deniability for principal domestic political leaders. The depth of information is another manifestation of McSherry's expert use of sources. At the individual level, the book provides names and insight into the personal characteristics of Condor's main leaders, planners and operatives. *Predatory States* is also painfully transparent regarding the culpability of mid-level and prominent U.S. government officials.

While the book is well referenced, the manner in which McSherry framed *Predatory States* ensures the narrative

misses an important aspect regarding the story of political violence in Latin American. The book's noticeable lack of historical reference to Latin America's unique social and cultural violence — independent of U.S. involvement — is disappointing. A Peruvian military massacre of 69 innocents in Accomarca in August 1985 during the state's internal conflict with the Shining Path is no outlier. Leftist party manifestos throughout the region during the period espoused a strategy reliant on insurrection and violent social revolution. Insurrectionist groups and political parties bluntly claimed their goal of total social, political, and economic transformation could not be achieved through democratic means. Revolutionaries targeted civilian populations as well, carrying out terror campaigns in urban environments. Yet the author omits reference to any leftist blame in Latin America's repertoire of political violence. Leftist use of underhanded tactics doesn't excuse the brutal reality of systematic and violent state repression. Painting Latin American revolutionaries as noble, and focused on social justice is an oversimplification.

All that said, the strengths of *Predatory States* outweigh its shortcomings. Two distinct audiences should consider reading it. First, undergraduate and graduate students of Latin American affairs, particularly the latter, looking to conduct worthwhile research projects would do well to emulate the

author's research methodology. Second, military service members, students of civil-military relations and policymakers considering how to best match national and defense strategy to current threats. Counterinsurgency and the employment of special capabilities will not soon disappear in the new era of great power competition; in fact, capacity in hybrid and asymmetric domains is once again proving critical. No matter the threat, consideration must always be given to the ethical employment of all elements of national power. 



## BOOK DETAILS

By **J. Patrice McSherry**

Lanham, Maryland: Rowman and Littlefield Publishers, Inc.,

2005, 285 pages;

ISBN: 978-0742536876

Price: \$37.95

## REVIEWED BY

**Major Corey Keiffer**

Psychological Operations  
Officer, currently attending the  
Naval Postgraduate School.

DEPARTMENT OF THE ARMY  
JFK SPECIAL WARFARE CENTER AND SCHOOL  
ATTN: ADJK-PAO  
3004 ARDENNES STREET, STOP A  
FORT BRAGG, NC 28310-9610

This publication is approved for public release; distribution is unlimited • Headquarters, Department of the Army • PB 80-21-2

**TECHNICAL EXPLOITATION COURSE | FORT BRAGG, NORTH CAROLINA**



U.S. ARMY PHOTO BY K. KASSENS | PIN: 211071-000