Cognitive-Emotional Conflict

Adversary Will and Social Resilience

By Linton Wells II

Today's information sharing tools let adversaries interfere more directly than ever with a targeted nation's political processes and the minds of its citizens.[1] Operating effectively in such "cognitive-emotional conflict" requires that information-based capabilities be employed and countered in agile, integrated ways across the military, government, and society.[2] Coherent narratives tied to strategy and backed by actions are important.[3] Technical cyberspace activities need to be well-coordinated with content-based approaches like military information operations, government-wide messaging, and intelligence gathering (including all forms of security).[4] Even more important is to build a society's resilience against persistent, disruptive, or disinformation campaigns that aim to undermine citizen confidence and core beliefs.[5]

The need for effective messaging is nothing new—targeting the minds of opposing leaders and the morale of their forces has been central to warfare from time immemorial. Historically, galvanizing public opinion in democracies usually has taken dramatic acts, from the Boston Massacre, to Pearl Harbor, to 9/11. Less dramatically, waning public opinion led President Bush to the Surge in Iraq, and President Obama to adjust his approach in Afghanistan. Activists today, however, have much more direct access to growing numbers of citizens, either to advocate for positions, muddy the waters of public opinion with alternative facts and fake news, or leak secrets to wide audiences. Empowered individuals and small groups can leverage media to enhance their impact by ensuring their asymmetric actions against people, societal structures, or military forces are much more widely disseminated. Some information activities will involve cyberspace operations, while some will involve more traditional information means. In any case, government communication tools such as press releases, white papers, web posts, or even leadership speeches rarely are effective counters to these information flows, especially when poorly coordinated.

The U.S. military and intelligence communities are starting to integrate their capabilities better, but implementing whole-of-government approaches is proving much harder owing to diverse interests, capabilities, and understandings of the information environment. Strengthening society's overall resilience to such campaigns is

Dr. Linton Wells II is a Visiting Distinguished Research Fellow at National Defense University. A retired U.S. Navy officer with more than five decades of public service, Dr. Wells served as Deputy Under Secretary of Defense and twice as Principal Deputy Assistant Secretary of Defense.

even more difficult, and also more important. A variety of reasons, from lack of trust to lack of capability, make it hard for most Western governments to craft and promote effective resilience campaigns. That said, transparency ultimately is a powerful asset, and where checks and balances, horizontal information flows, and citizen engagement exists, societies can adapt and become more resilient to cognitive-emotional attacks. However, the Strategic Multi-Layer Assessment (SMA) and others are doing important work on fake news inoculation and enhancing population resilience, as well as the use of neuroscience to help understand subconscious decisionmaking.[6] Positive steps to reframe and refocus arguments can be used to counter disinformation campaign tactics.[7]

The Continuum of Conflict

Where does cognitive-emotional conflict fit into the broader continuum of conflict that exists today? First one must define the continuum. Strategist Frank Hoffman at National Defense University defines this as measures ranging from "short of armed conflict" to "major theater war."[8] The spectrum includes an "unconventional and special warfare" category that cuts across the entire continuum of violence.[9] Most of the conflicts today fall into the blue and green zones identified in Figure 1.

Measures Short of Armed Conflict

A proposed definition is the employment of covert or illegal activities that are below the threshold of violence. This includes disruption of order, political subversion of government or non-governmental organizations, psychological operations, abuse of jurisprudence, and financial corruption as part of an integrated design to achieve strategic advantage.[10]

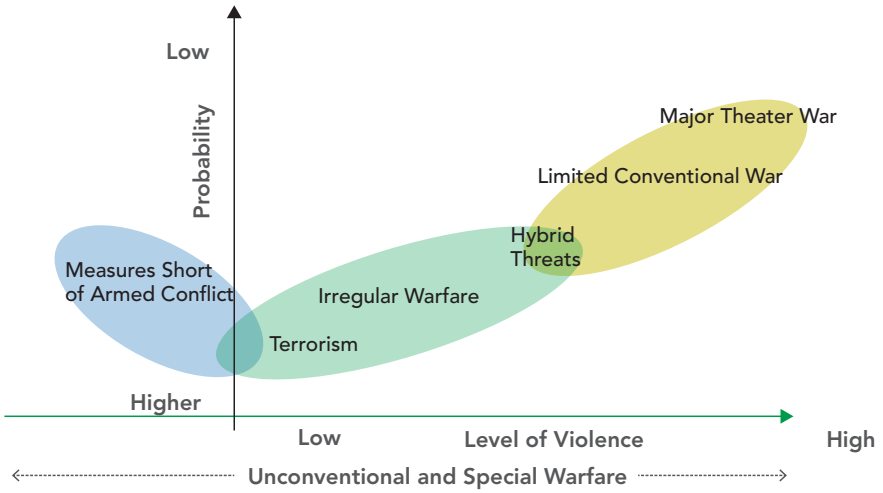
Irregular Warfare and Terrorism

Existing U.S. doctrine defines irregular warfare as a "violent struggle among state and non-state actors for legitimacy and influence over the relevant populations."[11] Irregular warfare is characterized by indirect and asymmetric approaches that avoid direct and risky confrontations with strong forces.[12] Irregular warfare may include criminal activity and/or terrorism.

Hybrid Threats

Hoffman defines this group as the "tailored violent application of advanced conventional military

FIGURE 1: Continuum of Conflict.



capabilities with irregular tactics, or combination of forces during armed conflict."[13]

Theories of Conflict and Resilience

War is "an act of force to compel the enemy to do your will"—fair enough, but a complementary formulation is "… supreme excellence [in war] consists in breaking the enemy's resistance without fighting."[14] Within the continuum of conflict, breaking the resistance of *both* civilian and military adversaries without fighting major wars is an increasingly common objective.

Key arguments in this area were introduced by John Arquilla and David Ronfeldt in their 1993 article "Cyberwar is Coming!"[15] that first introduced the concept of "cyberwar"—"the idea that the vulnerability of communications could cripple an advanced army" by "disrupting, if not destroying, information and communication systems…on which an adversary relies in order to *know itself*…"[16] Cyberwar has proven hard to define, and is not included in the official U.S. military lexicon, but "cyberspace operations" are, and they are associated with powerful technical components, usually considered to be offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and computer network exploitation (CNE).[17] Such operations can impact most conflicts, but often they have been treated as technical capabilities injected from a parallel, networked universe, rather than integrated as part of an overall campaign. However, Arquilla's and Ronfeldt's seminal 1993 article not only discussed how the information age is altering the nature of all conflict, but also introduced the concept of "netwar" in which actors seek to "disrupt, damage, or modify what a target population knows or thinks it knows about the world around it."[18] Today cyberspace operations closely relate to cyberwar with potential impacts on military systems, critical infrastructures, etc., while netwar is increasingly relevant to the cognitive and emotional disruption of societies.[19]

Worldwide, hundreds of billions of dollars are spent to defeat enemies on high-intensity battlefields. Such capabilities are necessary, but insufficient. A variety of cognitive-emotional campaigns are underway, from sustained efforts to undermine respect for liberal democratic values, to initiatives to establish new geopolitical "facts" in East Asian waters. Those suggest that the center of gravity for at least some conflicts is shifting away from military forces toward the political processes, thought leaders, and social media of the targeted populations. Rather than inciting a population to take a particular action, as the leak of the Zimmerman telegram did in accelerating the U.S. entry into World War I, campaigns today often seek to fragment citizen opinions and disrupt belief systems. The ultimate resilience of a nation or an alliance lies in the minds of its citizens who today are under persistent pressure.

There are many definitions of resilience, the best of which include proactive pre-crisis preparations and risk mitigation, effective incident management, and leveraging whatever shocks occur to build back better, as probability scholar Nassim Taleb advocates in his work, *Anti-Fragile: Things That Gain From Disorder.*[20] The Rockefeller Foundation defines resilience as:

> *The capacity of individuals, communities and systems to survive, adapt, and grow in the face of stress and shocks, and even transform when conditions require it. Building resilience is about making people, communities and systems better prepared to withstand catastrophic events—both natural and manmade—and able to bounce back more quickly and emerge stronger from these shocks and stresses.*[21]

The summary of resilience should therefore move from "bounce back" to "be prepared to bounce forward better."[22] How to strengthen the resilience of societies deserves more attention in conflict studies.

Cognitive-Emotional Conflict

Continued, long-term campaigns of disruption, perception management, and deception sow confusion and undercut values and convictions.[23] These campaigns are but one element of cognitive-emotional conflict. Many of their components are not new. They involve violence and the threat of violence, integrating kinetic and non-kinetic elements in ways that would be fully understood by Sun Tzu, Clausewitz, or John Boyd.

The American way of war historically has favored kinetic approaches in environments that clearly distinguish between combat and non-combat, where "one side distinctively wins while the other distinctively loses."[24] Violent action and its connection to policy have long been at the heart of Western military thought, but there also are complementary strategies. Sun Tzu did not clearly delineate between a state of peace and war, though violence and the threat of violence were part of his conception of statesmanship.[25] He did emphasize the importance of deception, perhaps since it helped the leader to "flow" between various states of conflict. Twentieth century military strategist John Boyd later addressed both the offensive and defensive sides of cognitive approaches, noting that strategy should "magnify and augment our inner spirit and strength" while swaying the uncommitted. It should also "isolate adversaries from their allies…[and from] one another, in order to magnify their internal friction, produce paralysis, bring about their collapse…so that they can no longer inhibit our vitality and growth."[26]

Information-based acts in cognitive conflict draw on many tools to "confuse, befuddle, discourage, confound, depress, deny, destroy, degrade, disrupt, usurp, corrupt, deter/dissuade, disconnect, cost-impose, dispose, convey weakness or worse, engender fear (or respect), herd/vector in desired direction and generally negatively impact on victims'/adversaries' ability to see, know, understand, command/control/access his own means, decide, act and be confident of his/her posture, processes or destiny… [These] actions will likely be applied around critical times."[27] Clearly they have been employed before in high-intensity wars (the deception operations surrounding Normandy), other armed conflicts (direct adversary messaging to populations during the Vietnam War and the First Intifada), and in measures short of armed conflict (propaganda and false news to undermine the legitimacy of governments or belief systems).

What is new today is the ease by which modern communications allow adversaries to bypass military forces, borders, and alliances to magnify their voices in the minds of our people, our adversaries, the uncommitted, and our allies.[28] Since experiencing disappointing results in Chechnya in the 1990s the Russians have been refining their "information-psychological" capabilities, which approximate the goals of netwar.[29] Parts of China's "three [unconventional] warfares" relate to efforts to implement "political work."[30] As future cyberspace activities evolve to destroy physical systems more effectively or disrupt essential services, they provide other ways to undercut the confidence of people in their governments.

There is an ample theoretical basis, and a range of operational capabilities, to support a portfolio of cognitive-emotional strategies, from offensive ones to influence opponents, to persuasive ones to encourage neutrality, to defensive ones to build cohesion. This is broader than a cognitive-emotional campaign in the military sense since key parts fall outside military control. Cognitive-emotional conflict is:

> *A struggle to affect the thoughts and values of people at all levels of an opponent's organization and society, using technical and other informational means, while preserving the resilience of one's own organizations and society, and attracting the uncommitted.*

Within this struggle of understanding an adversary's conscious and unconscious perceptions is the recognition that the process of creating actions to shape perceptions will be iterative. The next step is creating and highlighting mismatches in perceptions and using them as weaponized information to target the mind of the adversary and related populations.[31] Since it is impossible to understand perfectly how an adversary's perceptions can be shaped, messages will need to be tested continuously for effectiveness and adapted. Cognitive-emotional conflict thus extends across the entire continuum of conflict, as shown in Figure 2.

U.S. Advantages and Disadvantages in Cognitive-Emotional Conflict

Daunting as the military challenges may be, there are two greater problems: first, how to address coordination beyond the Department of Defense (DOD) in a whole-of-government framework? And then, how to move beyond government to achieve the kind of "whole-of-society" resilience that the nation, and its alliance partners, will need to face the coming cognitive-emotional challenges? The United States starts with a number of advantages, but also serious weaknesses.

U.S. Advantages in Cognitive-Emotional Conflict

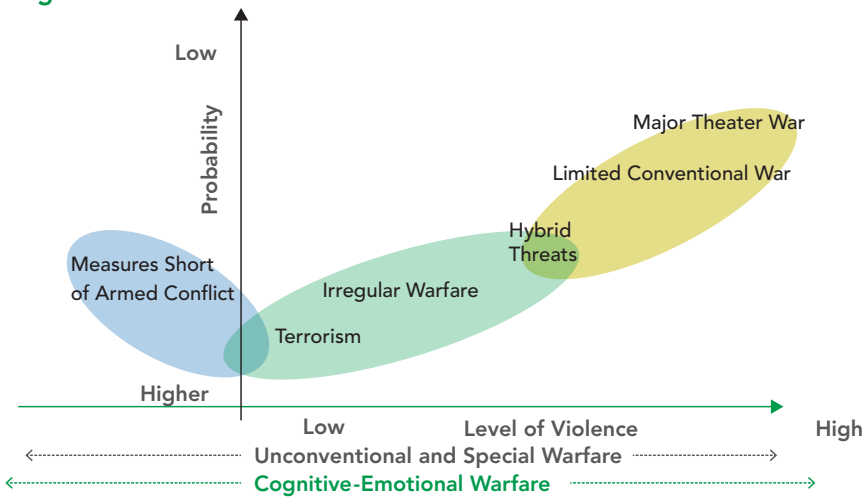
Military/Government Levels

DOD and the Intelligence Community (IC) have exceptional technical cyber capabilities across the full range of OCO, DCO, and CNE as well as many of the non-cyber disciplines, to include electronic warfare, operational deception, space, and command and control. Additionally, Special Operations Forces and parts of the cyber community can adapt quickly to emerging technology and changing circumstances. The U.S. hacking community also is more integrated into the cybersecurity community than in many other countries, partnering through programs like "bugs for bounty" and hackathons.

National Levels

Our diverse population and relatively open system is able to adapt in complex, uncertain environments. Many studies suggest that closed systems begin to lose their adaptability under adversity, and eventually come to be at risk of survival. Such closure can occur either through top down direction (such as isolating a national internet), or a self-selecting series of actions, such as choosing only reinforcing information sources (echo chambers) that limit understanding of a rapidly evolving environment.

FIGURE 2: Cognitive-Emotional Conflict Extends Across the Entire Continuum of Conflict.



Former Dean of Princeton's Woodrow Wilson School of Public and International Affairs, Anne Marie Slaughter, observed in 2009 that the United States ought to have significant advantages in a networked world that derive from the heterogeneity of its population, its geographic location, a horizontal social structure, and a culture of entrepreneurship and innovation.[32]

> *In a networked world, the United States has the potential to be the most connected country…If it pursues the right policies, the United States has the capacity and the cultural capital to reinvent itself.*

The United States possesses the checks and balances, diversity, and feedback loops, and is resilient enough to absorb lessons, learn from them, and adapt. A key is to recognize that "the antidote to netwar poison is active transparency," however painful and disruptive that may be to implement.[33]

U.S. Disadvantages in Cognitive Conflict

The exceptional increases anticipated in science and technology capabilities during the next 15 years will have social impacts as well as operational and strategic ones. Many technology fields such as biotech, robotics, information, nanotech, energy, and additive manufacturing are rapidly changing in parallel. These issues affect the winners and losers in society, the way nations interact, and the way our children think. They raise questions for policymakers, ambassadors, commanders, not just technical specialists. Technological changes, and their interactions, need to be considered as strategic variables in national security planning, but they rarely are today.[34]

Military/Government Levels

The United States and its allies, are not organized, trained, and equipped to be agile and effective in cognitive-emotional conflicts today.[35] U.S. military strengths and doctrine have been aligned more with conventional kinetic conflict than with nuanced cognitive-emotional approaches. Achieving integrated effects at strategic, operational, and even tactical levels is complicated by the way the U.S. now separates cyberspace operations, military information support operations (MISO), intelligence, civil affairs, and related fields into discrete disciplines with distinctive organizations, personnel systems, and operational concepts.[36] Though they often are intended to be mutually supporting, campaigns in each of these areas now may not interact as much as they should to produce integrated effects. Often they are executed at very different levels of classification by skilled operators who are doing their best, but who may be largely unaware of each other's needs and accomplishments.

The problem is compounded by how critical information flows increasingly are outside the government's control—for example, products of geographic information systems (GIS) from sources like commercial satellite imagery and unmanned systems—aerial, ground, and underwater. These are augmented by an explosion of new sensors, from smart phones to augmented reality devices, to the Internet of Things. Finally there is the volume, velocity, veracity, and value of information (IV4) produced by the 24/7 news cycle, amplified and accelerated by social media.

National Level

Most Americans do not recognize the threats posed by cognitive-emotional conflicts and weaponized information. Despite the nation's diversity, most Americans are poorly equipped, through language skills or cultural awareness, to engage deeply in foreign cultures.[37] This can make it hard to recognize that different nation states have different views of concepts such as soft power.[38] For example, Russia thinks of soft power as everything short of outright war (deception, fake news, etc.), while the United States

often views soft power as something that attracts people to American ideals.[39] Such differences make it hard to project, or counter, narratives effectively in foreign environments; particularly given how the United States has cognitive-emotional conflict needs that extend globally, but few of our allies can execute cognitive campaigns beyond regional levels.

The United States thus far has given insufficient attention to crafting and disseminating compelling narratives that shape perceptions. We have allowed our once exceptional capabilities for cognitive-emotional conflict—e.g. in the information campaigns of World War II and the activities of organizations like the U.S. Information Agency during the Cold War—to atrophy, and we lack a consistent national narrative to tell our story. Additionally, U.S. practitioners are bound by asymmetric legal, moral, and ethical constraints that often keep them from being agile enough to compete effectively with skilled adversaries in the realm of social media. This admittedly is a complex problem for any open, democratic society that does not perceive an existential threat.[40]

Consider how Russia's state-owned news outlets routinely deliver government-sponsored messages that are increasingly being accepted as unbiased.[41] And al-Qaeda in Iraq did not need to match U.S. armor or firepower. It only needed to record improvised explosive device (IED) attacks for broadcast to the world. It is much easier to kill one American and broadcast the video to millions than it is to try to kill ten thousand Americans in a combined arms maneuver campaign. Effective cognitive-emotional conflict amplifies small events to create effects in the adversary's mind. Daesh has leveraged these techniques through social media and has broadened its appeal to new regions such as Southeast Asia much more rapidly than expected.[42]

U.S. practitioners of cognitive-emotional conflict need excellent situational awareness, supported by securely networked systems and processes with information flowing as freely as possible, even while trying to disrupt and isolate adversary equivalents. The stovepipes among U.S. tools for cognitive-emotional conflict may be understandable, but they cannot deliver integrated effects. Other nations have fewer artificial restrictions. For example, the Russians, like the Soviets before them, do not separate the intelligence, operations, and communications functions, but rather refer to a more integrated "radio-electronic struggle," which avoids many of the inefficiencies caused by divisions among personnel structures, doctrine, management, etc. These are part of whole-of-government approaches.

Improving the Odds of Success in Cognitive-Emotional Conflict

Some suggest that we are reaching the end of the post–World War II international security structure, pressured by the challenges of a risen China, the resurgence of Russia, worldwide migration, and terrorism, and the various national and transnational responses.[43] The emerging structure is not yet clear, but cognitive and emotional elements certainly will be part of any follow-on conflicts. This section addresses the military, whole-of government, and societal actions that could help prepare for cognitive-emotional conflict in our changing world.

Information as a Joint Warfare Function

In July 2017, Chairman of the Joint Chiefs of Staff, General Joseph F. Dunford, Jr., approved the designation of information as the seventh joint warfare function.[44] This designation of information as the seventh joint warfare function opens up possibilities for coordination that are just now beginning to be examined. A strategy for "Operations in the Information Environment" (OIE) was issued almost one year prior, so there is a basis for considering the closer integration of cyber and content along the full spectrum of doctrine, organization, training, material, logistics, personnel, and facilities—better known as DOTMLPF. Other information-based

components that could benefit from closer integration include but are not limited to:

- strategic communications;
- electronic warfare, to include an electromagnetic pulse (EMP) attack;
- kinetic and non-kinetic operations;
- space and counter-space operations;
- operational security (OPSEC);
- military information support operations (MISO), a.k.a. PSYOPS;
- covert action/propaganda;
- controlled and uncontrolled leaks.[45]

These activities involve different skill sets, agencies, armed services, and even organizational cultures, and should include the Intelligence Community. Half steps are unlikely to be effective but, at the same time, trying to eat the whole elephant at once is likely to be overwhelming. First steps should focus on cross-cutting approaches to a few problems to maximize prospects for near-term successes. On the personnel side, recognize that not everyone will be able to perform well in this environment. Train and educate as broadly as possible, but focus on building a core team of exceptional practitioners.

Already the U.S. Navy has combined its intelligence (N2) and communications (N6) functions into an Information Warfare corps. Could/should similar functions be included by other armed services to improve integration and agility? Ironically, the potential split of U.S. Cyber Command from the National Security Agency may complicate these efforts to breakdown stovepipes.[46]

Alternatively, some have suggested that a new "Joint Concept for Cognitive-Emotional Warfare" be developed to give the idea of cognitive-emotional conflict a larger role in the training, budgetary, and force structure processes. Given the ongoing developments, this probably is premature. The other activities should be allowed to mature.

Reshaping the Broader U.S. Government for Cognitive-Emotional Conflict

The nation needs to convey, by all possible means, the narratives it seeks to represent it. Diplomacy—especially public diplomacy—is on the front line of this campaign, supported by aid programs, and the myriad of other messages the United States projects on a daily basis. Executive Branch departments other than Defense and State have important roles to play, as does industry.

The Department of Homeland Security (DHS), for example, is responsible for protecting the .gov domain and critical infrastructure. DHS has well-defined, whole-of-government management structures in-place for steady state and incident response activities.[47] These structures require collaboration with the private sector through mechanisms such as Information Sharing and Analysis Centers (ISACs) and Organizations (ISAOs), and response to a cyber incident could well be an important part of a cognitive conflict campaign.

Communications need to be aligned with strategy, which must be supported by both narrative and action.[48] Distorted information in a disinformation campaign can be reframed, refocusing can counter distraction, reaffirmation can offset dismissive efforts, and reassurance can address information intended to dismay.

Coordinating these activities is likely to be difficult, given the lack of an agreed U.S. national narrative at present, but it must be tried. Democracies have the added challenge of using information legally and ethically within severe constraints, which often are strained in cognitive-emotional conflict. Decisionmakers have no right to be wrong.

Increasing National Resilience against Cognitive-Emotional Conflict

Government action alone is unlikely to resolve key societal issues, given countervailing moral, legal, and ethical interpretations, as well as suspicions

of the government in many quarters. For example, legal and privacy concerns are critical elements of a democratic society, and they need thorough vetting, even though this may impede rapid action on cybersecurity issues. Impassioned policy discussions over security and privacy have existed since the beginning of the internet, and doubtless will continue in new directions as technology continues to evolve. No one side has all the answers, but the debates are essential, and are a far better approach than top down unitary, directed solutions.

Singapore has postulated a "total defense" concept involving military, civil, economic, social, and psychological components.[49] It recognizes citizen participation as essential as connectivity increases and infrastructures become more interdependent. Signs like "our diversity is our strength" are omnipresent across Singapore. Not every nation can match the tight integration of Singapore's population and their general trust in government. However, as noted earlier, nations that have strong systems of checks and balances, feedback loops, and open information flows have great sources of resilience. These should be nurtured, for they are the basis by which the nation can absorb cognitive-emotional attacks and adjust, over time, to the cognitive-emotional campaigns against them.

At the same time, serious research is needed into the basis of, and limits to, societal resilience in a networked world, especially in democracies. For example, what will be the likely impacts on resilience of disruptions of services through cyberattacks on infrastructures? What differentiates a spirited divergence of views from unbridgeable divisions of worldview? In some cases, neuroscience may be able to provide insights.[50] As these are being worked out, the critical importance of transparency remains. The adjustments are not likely to be quick, smooth, or painless, but they must happen, and represent one of the nation's greatest strengths in cognitive-emotional conflict.

Parting Thoughts

Today's environment is particularly conducive to cognitive-emotional conflicts, owing to the rise of cyber interconnectedness and the range and reach of information sharing tools. There are billions of netizens and billions more will connect during the next few years. This level of connectedness accelerates change and can disrupt many of the policy formulation mechanisms that are legacies of the industrial age, "When decision-makers had time to study a specific issue and develop the necessary response or appropriate regulatory framework."[51] Cognitive-emotional conflict thrives in this dynamic, interconnected environment, and the "weaponization of information" is one way that it can challenge the established order. Actions, both violent and non-violent, can be tailored for nearly instant network dissemination. The nimble player who can shape perceptions generally wins against slow and methodical one.

Success in these sorts of contests requires the nimble, nuanced, and harmonized use, not only of all aspects of national power, but also of non-state and transnational instruments.[52] Strategy, narrative, and actions need to be aligned. Cyberspace operations need to be integrated with "other information-based attacks, defenses, or exploitations as a means for conveying influence, signaling, messaging, or executing strategic communications based on the information-based content itself."[53] All must be supported by intelligence attuned to each area. Decisionmakers and their staffs will need near-real-time situational awareness, yet with options that provide time for reflection. Parts of an engagement will proceed at machine speed with people "on-the-loop," rather than "in-the-loop," while other aspects will require nuanced cultural understanding, sophisticated narratives, and human contact.[54] Throughout, citizens must be informed in credible ways, amidst myriad countervailing information flows, many of them ill-informed at

best, and malicious at worst. Conspiracy theories abound, amplified by information "echo chambers."[55] No organization today—government or civilian—is prepared to deal with all these forces effectively in real-time. PRISM

Notes

[1] This paper represents my personal views and does not reflect the opinions of National Defense University or the U.S. Government. It would not have been completed without major contributions by Maj Phillip Lere, USAF. Dr. Frank Hoffman, Dr. T.X. Hammes, and ADM William O. Studeman, USN (ret.), and Dr. Rebecca Goolsby provided invaluable insights. Any errors are my own.

[2] Cognitive processes involve the acquisition and understanding of knowledge which, while important, are not sufficient to address the full scope of emotions targeted by today's information and disinformation campaigns.

[3] Mark Laity, Director of Strategic Communications at NATO's Allied Command Operations (ACO) repeatedly made this point to a roundtable of senior Southeastern European (SEE) leaders on September 27, 2017.

[4] Cognitive-emotional conflict is defined later in this article. Information Operations are defined in U.S. Joint Publication (JP) 3–13 as "the integrated employment, during military operations, of IRCs [information related capabilities] in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own." JP–3-13, November 27, 2012 incorporating Change 1, November 20, 2014, ix. This definition makes it clear that IO primarily applies to military operations, although the "in concert with other lines of effort" could tie into "whole-of-government," or even "whole-of-society" conflicts. For more information see <http://dtic.mil/doctrine/new_pubs/jp3_13.pdf>. RAND notes IO and IW "… also known as influence operations, includes the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent." For more information see <https://www.rand.org/topics/information-operations.html>.

[5] Resilience is defined later in this article.

[6] From the SMA description: "The Strategic Multi-Layer Assessment (SMA) provides planning support to Commands with complex operational imperatives requiring multi-agency, multi-disciplinary solutions that are NOT within core Service/Agency competency. Solutions and participants are sought across USG and beyond. SMA is accepted and synchronized by the Joint Staff/J-39 Deputy Director for Global Operations (DDGO) and executed by the Deputy Assistant Secretary of Defense (DASD) for Emerging Challenges and Prototyping (EC&P).

See, for example SMA Panel Discussion: Fake News Inoculation and Enhanced Population Resilience, a Department of State Perspective; Booklet July 6, 2017.

[7] Dr. Rebecca Goolsby proposes four "Rs" (reframe, refocus, reaffirm and reassure) to counter the four "D"s of disinformation campaigns (distort, distract, dismiss, dismay). Presentation to a roundtable of senior Southeastern European (SEE) leaders on September 26, 2017.

[8] F.G. Hoffman, Exploring a Continuum of Contemporary Conflict, December 2016, unpublished.

[9] Unconventional warfare (UW) is defined by U.S. doctrine as "activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow an occupying power or government by operating through or with an underground, auxiliary, and guerrilla force in a denied area." JP 3–14, *Unconventional Warfare*, September 2015. This mode of conflict is usually done covertly, with low signatures and limited footprint, and conducted primarily by Special Operations forces.

[10] Hoffman, working definition. In his formulation, "Measures Short of Armed Conflict" include so-called "gray zone" operations, which now are not clearly defined in doctrine. That said, others have provided working definitions of "gray zone activity" as "an adversary's purposeful use of single of multiple elements of power to achieve security objectives by way of activities that are typically ambiguous or cloud attribution, and exceed the threshold of ordinary competition, yet intentionally fall below the level of open warfare." U.S. Strategic Multi-Level Assessment (SMA) Gray Zone Effort Update, February 2017, 1. Special Operations Command (SOCOM) has used "Competition Short of Armed Conflict" (CSAC) in lieu of MSAC, ibid, 3.

[11] First established in the Joint Staff (J7) *Irregular Warfare Joint Operating Concept*, version 1.0, Washington D.C., September 11, 2007.

[12] Irregular Warfare often is abbreviated IW, which is confusing in the context of this paper with Information Warfare. Accordingly, "IW" in this paper only refers to Information Warfare.

[13] Hoffman, 19.

[14] Carl Von. Clausewitz, *On War*, translated by Michael Howard and Peter Paret, Princeton University Press,1976, 75. Sun Tsu *The Art of War*, translated by Lionel Giles, Amazon Classics, 2017, available at <https://www.amazon.com/Art-War-AmazonClassics-Sun-Tzu/dp/1542047528/ref=sr_1_3?s=books&ie=UTF8&qid=1502664791&sr=1-3&keywords=art+of+war>. This is a more nuanced formulation than what is sometimes translated as to "defeat an enemy without fighting is the acme of skill."

[15] John Arquilla and David Ronfeldt, "Cyberwar is Coming!," *Comparative Strategy*, Volume 12, Number 2 (1993): 144¬46. Precise definition is used by Arquilla in his interview with FRONTLINE on March 4, 2003, available at < http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html>.

[16] Ibid,146.

[17] *Cyber Operations*, JP3–12(R), February 5, 2013,vii and I–3.

[18] Cited in Robert Brose. "Cyber War, Netwar, and the Future of Cyberdefense" DNI, 2012 available at <https://www.dni.gov/files/documents/atf/Cyber%20War%20Netwar%20and%20the%20Future%20of%20Cyberdefense_Header.pdf>, 2-3, et. seq.(emphasis supplied).

[19] John Arquilla and David Ronfeldt, "Cyberwar is Coming!," *Comparative Strategy*, Vol 12, No 2 (1993), 144. Cited in Robert Brose. "Cyber War, Netwar, and the Future of Cyberdefense," 2012, available at <https://www.dni.gov/files/documents/atf/Cyber%20War%20Netwar%20and%20the%20Future%20of%20Cyberdefense_Header.pdf>, 2–3, et. seq.

[20] Nassim Taleb, *Anti-Fragile: Things That Gain from Disorder*, 2014, available at <https://www.amazon.com/dp/B0083DJWGO/ref=dp-kindle-redirect?_encoding=UTF8&btkr=1>.

[21] Rockerfeller Foundation, "Valuing the Resilience Dividend: A New Way Forward," available at <https://www.rockefellerfoundation.org/our-work/topics/resilience/>.

[22] I am indebted to Dr. Dane Egli for his insights about this formulation.

[23] A speaker in Singapore recently referred to this as "slow burn" threats that erode public unity and confidence: Lin Qinghui briefing at the Asia-Pacific Programme for Senior Military Officers (APPSMO), Singapore, August 8, 2017.

[24] CAPT Phil Kapusta, USN, in SMA "Panel Discussion on the Gray Zone in support of USSOCOM," April 27, 2017, 4.

[25] Michael I. Handel, *Masters of War: Classical Strategic Thought*. London: Routledge, 3rd edition, 2000.

[26] Frans Osinga, Science, *Strategy and War: the Strategic Theory of John Boyd*. London: Routledge, 2007, 213.

[27] ADM William O. Studeman, USN (ret.) "Tutorial on Managing the Overlap Between and Alignment of Cyber, Information Warfare/Conflict/Operations and Intelligence (including all forms of security)," February 2017. Critical times include elections, preparation for military operations, during campaigns to build public support, etc.

[28] Osinga op. cit.

[29] Brose, op. cit., 10–11. The complement of "Information-Psychological" capabilities is "Information-Technical" efforts, which equate more to cyberwar.

[30] *Ibid*, 18–23.

[31] Rand Waltzman, "The Weaponization of Information: The Need for Cognitive Security," testimony before the Senate Armed Services Committee, Subcommittee on Cybersecurity on April 27, 2017, available at <https://www.armed-services.senate.gov/imo/media/doc/Waltzman_04-27-17.pdf>. Osinga, op. cit., 217.

[32] Anne-Marie Slaughter, "America's Edge: Power in the Networked Century," *Foreign Affairs*, January/February, 2009. Looking back, many aspects of this article now seem optimistic, but the points about the strengths the United States can derive from its diversity and networking seem valid.

[33] Brose, *op. cit*., 28.

[34] James Kadtke and Linton Wells II, "Technology Is a Strategic National Security Component," *Signal* Magazine, January 2015, available at <http://www.afcea.org/content/?q=node/13831>.

[35] Linton Wells II, "Prepared for Battle, But Not Prepared for War," *Proceedings*, (U.S. Naval Institute Press: November 2017).

[36] Military information support operations— Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives. Also called MISO. (JP 3–13.2), available at <http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf>.

[37] This extends beyond inabilities to speak foreign languages or unfamiliarity with the norms of other cultures. Richard E. Nisbett, in *The Geography of Thought: How Asians and Westerners Think Differently...and Why*, 2004, examines differences in basic thought processes between US/European and East Asian societies. During a recent Compexity Workshop in Singapore, Dr. Cheong Siew An, in a presentation entitled "Complex Narratives and Identities," noted the difficulty in aligning cultural narratives with historical facts.

[38] Brose, *op. cit*.,15.

[39] Joseph S. Nye, Jr., *Soft Power: The Means To Success In World Politics*, New York: Public Affairs, 2009.

[40] See, for example, CAPT Wayne Porter, TEDx talk "A National Strategic Narrative & Role of American Communities." May 18, 2014, available at <https://www.youtube.com/watch?v=BWO8JJcqrVs>and the broader, website available at <http://nationalstrategicnarrative.org/>.

[41] See, for example: Peter Pomerantsev, *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia*, Public Affairs, 2014; see also "Russia and the Menace of Unreality," *The Atlantic*, September 9, 2014, available at <http://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/>, accessed December 30, 2016.

[42] Jerard, "Índomitable Hydra," *op. cit.*

[43] Views expressed at Singapore's International Risk Assessment Horizon Scanning Symposium (IRAHSS), July 18–19, 2017.

[44] The U.S. military traditionally has recognized six warfare functions: Command and Control (C2), Intelligence, Fires, Movement and Maneuver, Protection, and Sustainment. A review of the National Military Strategy (NMS) this year led to an annex on "*Shaping the Joint Force*" that directed the joint force to "treat information as a joint function." Change 1 to Joint Publication 1, *Doctrine for the Armed Forces of the United States*, dated July 12, 2017, established information as the seventh joint function, available at <http://dtic.mil/doctrine/new_pubs/jp1_ch1.pdf>.

[45] Studeman, *op. cit.*

[46] Patrick Tucker, "What the Announced NSA/Cyber Command Split Means," *Defense One*, August 18, 2017, available at <http://www.defenseone.com/technology/2017/08/what-announced-nsa-cyber-command-split-means/140362/>.Based on other reporting, it is not clear the NSA/Cyber Command split has been finalized.

[47] See, for example, Linton Wells II, Motohiro Tsuchiya, and Riley Repko, Improving Cybersecurity Cooperation between the Governments of the United States and Japan <https://spfusa.org/wp-content/uploads/2017/02/Improved-Cybersecurity-cooperation.pdf>, 4–9.

[48] Laity , *op. cit.*

[49] Lin Qinghui briefing at Asia-Pacific Programme for Senior Military Officers (APPSMO), *op. cit*.

[50] SMA, "Leveraging Neuroscience for Understanding the Cognitive Battlefeld," August 2017.

[51] These conflicts are shaped by diverse, dynamic forces, from accelerating technological change, to the Fourth Industrial Revolution as postulated by Dr. Klaus Schwab of the World Economic Forum in: Klaus Schwab, "The Fourth Industrial Revolution: What it Means, How to Respond," January 14, 2016, available at <http://www.weforum.org/agenda/2016/01/>, accessed February 16, 2016. Many of these issues are beyond the scope of the Defense Department's role, but there are steps that DOD can take to help the nation deal with them.

[52] The rapid spread of jihadist ideologies in Southeast Asia during 2015–17 shows an exceptionally nimble, nuanced and integrated use of non-state and trans-national instruments. See Jolene Jerard, "Indomitable Hydra: Transnational Terrorist Threat," presented at the Military Studies Programme Seminar 2017 at the S. Rajaratnam School of International Studies

(RSIS), Nanyang Technological University, Singapore, August 11, 2017.

[53] Studeman, *op. cit*.

[54] "Man-in-the-loop" refers to situations where people make the key decisions. "Man-on-the-loop" recognizes that some aspects of modern warfare, notable machine-to-machine computer operations move too quickly for people to be engaged at every step and so the person ON the loop must pre-delegate certain ranges of action to the autonomous subsystems when certain criteria are met. This is equivalent to delegating authority under "rules of engagement."

[55] Information flows that reinforce each other to support a particular point of view, or world view, form an "echo chamber."