2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Cyberwar, Netwar, and the Future of Cyberdefense

Robert Brose
Office of the Director of National Intelligence[1]
Washington D.C., United States of America

Abstract: Over twenty years ago, Arquilla and Ronfeldt warned that both "Netwar" and "Cyberwar" were coming, and could impact the 21st Century security landscape as significantly as combined arms maneuver warfare had impacted the security landscape of the 20th. Since that time, the concept of "Cyberwar" has received great attention, while the parallel concept of "Netwar" has languished, even as its salience to global security has continued to grow. This paper suggests that just as Cyberdefense organizations have been required to confront Cyberwar, Netwar organizations, or Netwar-savvy Cyberdefense organizations, are increasingly needed to counter Netwar. Revisiting the Netwar concepts of the 1990s, it offers a 21st century Netwar definition; examines Netwar from a non-western perspective, exploring intersections between Netwar and Russian concepts of 'Information-Psychological,' Chinese United Front Theory, and Chinese Legal Warfare, and concludes with thoughts on unique roles that today's Cyberdefence organizations may play in future Netwar conflict.

Keywords: *cyberwar, netwar, information-psychological, united front theory*

1. INTRODUCTION

In the summer of 1993, a twenty-page article titled "Cyberwar is coming!" anticipated many of the challenges that western national security practitioners would encounter in years to follow. The paper featured an inspired emphasis on the socially-transforming effects of information technology suggesting "…the information revolution is strengthening the importance of all forms of networks, such as social networks…"[2]; anticipated that cyber-concepts could transform the role of militaries, imagining a day when militaries would conduct "hitting without holding"[3]; and included an eerie forecast of future crises' in which the U.S. might face "large, well-armed irregular forces, taking maximum advantage of familiar terrain, motivated by religious, ethnic, or tribal zeal… [and able to] move easily within and between the "membranes" of fractionated

1 The author of this paper is the Lead for Futures and Capability Development at the U.S. Office of the Director of National Intelligence (ODNI). The author prepared this work as a conceptual thought piece as part of his official U.S. Government duties. However, this paper should not be interpreted as an official policy, policy statement, or endorsement, either expressed or implied, of ODNI or the U.S. Government. This paper is a U.S. Government work. The U.S. Government hereby claims all applicable copyright protection under the laws of any country in which this paper is reproduced, published, or distributed.

2 John Arquilla and David Ronfeldt, *Cyberwar is Coming!* in COMPARATIVE STRATEGY, Vol. 12, No. 2, Spring 1993, pp. 141–165, 144.

3 *Id*. at 157.

states."[4] As the centerpiece of this article, authors John Arquilla and David Ronfeldt, then of the RAND Corporation but speaking on their own behalf, defined Cyberwar and Netwar as two emergent forms of warfare meriting greater study.[5]

Since that time, Cyberwar – the act of "disrupting, if not destroying, information and communication systems…on which an adversary relies in order to know itself…"[6] – has received substantial attention, from practitioners, policymakers, industry, and security theorists. However, if Cyberwar served as the bright 'Yang' of the paper, its' shadowy 'Yin' counterpart was Netwar, in which actors overtly and covertly sought to "…disrupt, damage, or modify what a target population knows or thinks it knows about the world around it."[7] It is this darker, less clearly bounded and potentially more profound challenge to the security of open and democratic nations that this paper focuses on in detail, first offering an updated definition of Netwar, then highlighting Russian and Chinese doctrinal concepts that may be applied in Netwar, and finally concluding with thoughts on how western actors may re-purpose or adapt traditional cyber organizations for Netwar defence.

2. NETWAR, THEN AND NOW

"Whereas Cyberwar refers to knowledge-related conflict at the military level, Netwar applies to societal struggles most often associated with low-intensity conflict…"[8]

The early concepts put forward by Arquilla and Ronfeldt focused for the most part on what they termed Cyberwar – impacts of emerging *network technologies* on conventional warfare, and the implications of attacks on the interdependence and transformative connectivity that would result. Of the twenty pages in the article, only a few address Netwar, and the thinking is less developed, but enough emerges from the document to make the following distinctions:[9]

1. Although it may be conducted in *concert with* Cyberwar, Netwar is qualitatively different from Cyberwar; while Cyberwar targets information systems, Netwar targets societal self- and world-perceptions;
2. Netwar may be pursued through any combination of diplomacy, propaganda, psychological campaigns, political and cultural subversion, deception or interference with local media, and efforts to promote dissident or opposition movements via computer networks;
3. Netwar may also involve infiltration of computer networks and databases, but if "this leads to targeting an enemy's military C3I capabilities" the action has crossed from Netwar to Cyberwar.

This thinking has since evolved and been refined by the global cyber security community (Arquilla and Ronfeldt included,) but the prevailing focus has remained Cyberwar. Martin Libicki, writing in *Strategic Studies Quarterly*, provides a refresh of the Cyberwar concept, but seems to view Cyberwar as an activity predominantly undertaken to support "combat in the physical domain,"[10] and the Tallinn Manual on the International Law Applicable to Cyber

4 *Id*. at 160.
5 *Id*. at 141.
6 *Id*. at 146.
7 *Id*. at 144.
8 *Id*. at 141.
9 *Id*. at 144-145.
10 Martin C. Libicki, *Why Cyber War Will Not and Should Not Have Its Grand Strategist*, STRATEGIC STUDIES QUARTERLY, Volume 8, No 1 (2014).

Warfare[11] defines 'Cyber' as the "networked technology" itself, 'warfare' as the "use of force," and acknowledges that it does not address cyber activities "below the level of 'use of force'."[12] Yet, would any national security scholar or practitioner dispute that at least some components of Netwar – for example, deliberate combinations of diplomacy, propaganda, and manipulation of media – seem to be growing in the modern geopolitical space? And do we not recognize an increasing potential for delivery of psychological campaigns to our doorstep, and the mobilization of 'dissident or opposition movements,' whether at the behest of state or non-state actors, via the Internet? If so, then we must also acknowledge that Netwar has in fact emerged alongside Cyberwar, and offer a definition of it that can enable a more effective and insightful analysis of current events than is possible without it.

3. A WORKING DEFINITION OF MODERN NETWAR

I offer the following as a working definition of Netwar in the 21st Century:

1. *Netwar consists of intentional activities to influence the domain of human perception via either overt or hidden channels, in which one or more actors seeks to impose a desired change upon the perception of another actor, in order that this change facilitate second-and third order effects of benefit to them;*
2. *Netwar does not imply a resort to physical force, non-cooperative modification of digital data, or even, necessarily, an act that violates any written laws of the targeted actor or the present-day international system;*[13]
3. *Discrete actions within a Netwar may include collective, personal, or machine-generated speech or action, economic choices, or other legally protected activities, in addition to acts of information conveyance, distortion, or denial that may or may not violate laws or sovereignty.*

This is a broad definition, not entirely discontinuous from US doctrinal descriptions of "Diplomatic, Informational, Military, and Economic" (DIME) power, and NATO descriptions of "Cyber operations" conducted as a component of "state power."[14] However, while Netwar may entail the use of cyber systems and tools as conduits, it is not "employment of cyber capabilities with the primary purpose of achieving [military] objectives,"[15] but instead the utilization of cyber (or social) systems as infrastructure supporting perceptual manipulation aimed at "achieving strategic goals."[16]

This broad definition also highlights the challenge of Netwar: employment of the 'M' in DIME may violate the UN Charter, intersect NATO article 5, or justify a range of 'out of band' responses, but a Netwar "attack" on target perceptions, conducted without attributable use of military force, presents the target with fewer internationally acceptable responses – particularly if they are unprepared, or unable, to respond via a Netwar of their own. It is this very asymmetry

11 Michael N. Schmitt (ed.), TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, United Kingdom, Cambridge University Press, 2013, 3.

12 *Id*, at 4.

13 Cyberwar activities of the 'Cyber-on-Cyber' variety – when they do occur – may facilitate Netwar, or be conducted in parallel to Netwar, as may be kinetic forms of warfare, but these are not acts of Netwar in and of themselves.

14 "Fighting Power, Targeting and Cyber Operations" in THE 6TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT PROCEEDINGS, NATO CCDCOE Publications, Tallinn, Estonia, 2014, 307.

15 Michael N. Schmitt, *supra* note 11 at 258, and in Paul Ducheine and Jelle van Haaster, *Id*. at 304.

16 Paul Ducheine and Jelle van Haaster, *Id*. at 305.

of means-legitimacy which a shrewd Netwar practitioner may exploit, and which the following sections explore.

4. NETWAR IN EASTERN PERSPECTIVE

While western national security practitioners may lack a "Grand Strategist" of Netwar, to paraphrase Martin Libicki,[17] their eastern counterparts have several to choose from. Qiao Liang and Wang Xiangsui's relatively recent treatise, *Unrestricted Warfare*[18], provides some hints at the deeper theoretical reservoir an eastern strategist might draw upon, but was perhaps better understood as a critique of U.S. – or extant Chinese – methods through an orientalist lens. As some western reviewers have noted, *Unrestricted Warfare* represented "neither a revolution in military thought nor an executable doctrine for future warfare but a collection of tactics, techniques, and procedures that have been used throughout history."[19]

For deeper insight, a modern day Netwar practitioner must look farther into the past. From the 64 discrete socio-political conditions described - albeit in semi-mystical terms - within the I-Ching, to the more widely read *Art of War* by Sun-Tzu, Oriental classics offer a wealth of anecdotally expressed thinking on how disparate influences may be brought to bear on an opponent, deflecting, co-opting, or "defeating" them without resort to physical violence. It has become cliché for western authors to cite Sun-Tzu's aphorism that "to defeat an enemy without fighting is the acme of skill,"[20] [21] and then treat the concept superficially, but the very words an English speaker employs in translation may distort the understanding of the concepts; in English defeat implies overthrow, downfall, conquest, and rout.[22] In contrast, study of Chinese history suggests Sun-Tzu would have likely included *any outcome that allowed the protagonist to significantly advance their interests* as a 'defeat' for the opponent, and recognized the possibility of 'opponent' to become ally or neutral party in an instant[23] (in other words, *it is the state of effective opposition*, not the entity themselves, that must necessarily be defeated.)

In the traditional eastern perspective every entity is perpetually vying for advantage within a sea of competitive forces, and competition with others is not a discrete (or moral) act to be initiated against a select set of 'bad guys' or 'evil-doers', but an eternally present and universal fact, which any rational actor denies at their peril. As George Kennan wrote, in describing the Soviet Union of 1947, *"...its political action is a fluid stream which moves constantly, wherever it is permitted to move, toward a given goal. Its main concern is to make sure that it has filled every nook and cranny available to it in the basin of world power. But if it finds unassailable barriers in its path, it accepts these philosophically and accommodates itself to*

17 Libicki, *supra* note 10.
18 Qiao Liang and Wang Xiangsui, UNRESTRICTED WARFARE, PLA Literature and Arts Publishing House, China, 1999.
19 Major John A. Van Messel, USMC, *Unrestricted Warfare: A Chinese doctrine for future warfare?* (Submitted in partial fulfillment of the requirements for the degree of Master of Operational Studies, United States Marine Corps School of Advanced Warfighting, 2005).
20 Dean Cheng, "Winning a War Without Fighting," THE WASHINGTON TIMES, July 19, 2013, accessed at http://www.heritage.org/research/commentary/2013/7/winning-a-war-without-fighting.
21 Arquilla and Ronfeldt themselves likely alluded to Sun-Tzu when they described Cyberwar as an act in which one disrupts means "an adversary relies in order to know itself…"
22 MICROSOFT Word Thesaurus (search for "defeat").
23 See various stories recounted in the Chinese classic ROMANCE OF THE THREE KINGDOMS, or 'San-Guo'

them."[24] From this perspective, "defeats" are seldom absolute, nor is a "victory" – or alliance - decisive. Thus, Sun-Tzu's aphorism might be alternately translated as 'the accomplishment of objectives through persistent persuasion, dissuasion, and manipulation is preferable to a resort to conflict in the physical domain' – a mission statement that seems well-aligned with the proposed definition of Netwar.

Strategists like Sun-Tzu are creatures of an ancient past, and at first glance, may seem several orders-removed from today, but if one looks at the 20th Century writings and actions of eastern powers, one can find concepts bridging the gap between these primeval concepts and the present. These include Russia's "Information Psychological," and the Chinese concepts of United Front Theory and Legal Warfare. Although each is different, they hold in common the basic premise that something resembling Netwar can and should be conducted in service of state objectives, and their study can serve as both tools to understand foreign perspective, and as concepts to inform modern Netwar.

5. INFORMATION-PSYCHOLOGICAL

"Excessive data do not enlighten the reader or the listener; they drown him. He cannot remember them all, or coordinate them, or understand them; if he does not want to risk losing his mind, he will merely draw a general picture from them. And the more facts supplied, the more simplistic the image…"[25]

Just as *Unrestricted Warfare* serves as a landmark for westerners seeking an entrée into the world of Chinese strategic thought, a recent article by Russian General Valery Gerasimov has of-late served to crystallize western awareness of asymmetric – or 'hybrid' - warfare as an emerging Russian forte. Writing in a 2013 issue of Voenno-promyshlennyi kur'er, or the *Military-Industrial Courier*, then Chief of the General Staff Gerasimov suggested that the "nonmilitary means of achieving political and strategic goals," which he characterized as "political, economic, informational, humanitarian, and other nonmilitary measures — applied in coordination with the protest potential of the population," were beginning to exceed traditional "kinetic" means in their net effectiveness.[26] Often referred to as the "Gerasimov Doctrine," this article has sometimes been described in the west as "prophetic"[27] in nature, but in reality merely summarizes and reframes the last fifteen years of evolution in Russian Military thinking. In his 2005 overview of global Information Operations concepts *Cyber Silhouettes*, Timothy Thomas noted that circa 2000, Russian military doctrine had already begun to differentiate between two forms of information conflict, acts of "Information Technical" and acts of "Information Psychological." *Information Technical* was associated with concepts that approximate today's western concepts of Cyberwar - "…technical intelligence devices, means and measures for protecting information, super-high-frequency weapons …radio-electronic

24 George F. Kennan, The Sources of Soviet Conduct quoted in Alexander J. Motyl *The Sources of Russian Conduct: the New Case for Containment*, FOREIGN AFFAIRS 16 November, 2014, accessed at http://www.foreignaffairs.com/articles/142366/alexander-j-motyl/the-sources-of-russian-conduct.

25 Jacques Ellul, Propaganda: The Formation of Men's Attitudes, New York: Knopf, 1965 on WIKIPEDIA accessed at http://en.wikipedia.org/wiki/Jacques_Ellul.

26 Valery Gerasimov, *The Value of Science in Prediction* in The 'Gerasimov Doctrine' and Russian Non-Linear War, by Mark Galeotti's blog "In Moscow's Shadows," accessed at https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

27 Sam Jones, Ukraine: *Russia's new art of war*, FINANCIAL TIMES, 28August 2014, accessed at http://www.ft.com/cms/s/2/ea5e82fa-2e0c-11e4-b760-00144feabdc0.html#axzz3TdT0UrNC.

countermeasures, electromagnetic impulse weapons, and special software and hardware."[28] In contrast, *Information Psychological* was associated with use of the mass-media, and with the employment of "nonlethal weapons, psychotronic tools, and special pharmaceuticals." While these latter exotica fall outside the scope of this paper, study suggests Russia is using the mass-media, per *Information Psychological*, in its historic and present-day conduct of Netwar.

Whatever capabilities of propaganda the Soviet Union may have built up in the years preceding, a robust *Information Psychological* capability was lacking during the early years of post-Soviet Russian state. During the 1994-1996 period of the Chechen conflict, the Russian military failed to take an active part in generating content to fill the global media space, and when it did communicate to the media, did so haphazardly.[29] Russian journalists – at the time still relatively free from state control[30] - received both preferential access, and even funding for minor expenses, from a Chechen community spanning national borders as they reported on the conflict. Meanwhile, Russia's Chechen adversaries deployed mobile television production teams to support a dedicated Ministry of Information. In the words of Russian Major General Zolotarev, "the Chechen campaign of 1994-1996 by military definition was three-quarters won by the Russian Army by August 1996, but by that time it had lost 100% in infospace."[31] It was this era of Netwar *failure* that drove the next stage in Russian thinking.

By 1999 – just before the emergence of *Information Psychological* in the open literature – Russia demonstrated an ability to execute at least components of a Netwar in Chechnya. The Russian military supplied videos and briefing material through centers established in areas that were serving as staging areas for Russian journalists in the neighboring republics of Dagestan and North Ossetia.[32] Russian authorities also censored any content deemed adversary propaganda, initially shutting off independent reporting, and then maintaining bans of certain types of content throughout the conflict.[33] By the end of 1999, a new centralized Russian Information Center (RIC) was filtering content from the theatre of operations, and information from any foreign publications to be disseminated inside Russia,[34] with relatively crude censorship approaches complemented by shaping of themes and the tone of coverage associated with the Russian military itself, at least when directed at the domestic population. Emil Pain, a Russian trained ethno-sociologist and an "advisor to the Russian Federation President since

28 Timothy Thomas, CYBER SILHOUETTES, Fort Leavenworth KS, Foreign Military Studies Office, 2005, 79.
29 *Id*. at 183.
30 *Id*. at 82.
31 *Id*. at 183.
32 *Id*. at 82.
33 *Id*. at 184.
34 The timing of RIC establishment *generally* coincides with both Vladimir Putin's assumption of the Presidency, and with a formal "Resolution 1538" (R-1538) of the Russian President. However, there is divergence in western accounts regarding the timing of both R-1538 and the stand-up of the RIC, raising the possibility that the "resolution" may have actually served to retroactively legitimize an *Information Psychological* fait-accompli. Thomas cites December of 1999 as the date for R-1538, and implies the RIC soon followed, while Paul Rich, writing in Crises in the Caucasus: Russia, Georgia, and the West (Routledge, 2013) claims the RIC was established by a "Governmental decree of 7 October." Suggesting even greater lag between RIC establishment and R-1538, French IO expert Daniel Ventre (who highlights the resolutions' parallel role in strengthening the powers of Russia's Federal Security Bureau) gives 7 February 2000 as the date of R-1538 [see Daniel Ventre, INFORMATION WARFARE, (United Kingdom, ISTE Ltd, and United States of America, John Wiley and Sons, 2009),] while Google's cache holds a 13 January 2000 *Voice of Russia* interview with *then RIC-head* Mikhail Margelov, stating that the RIC had been "opened on October 1st by the government."

1996,"[35] noted that by 2000, the very terminology used to describe the conflict had shifted. The Army was described as simply "working" in Chechnya, with the assaults it conducted termed "special operation[s]." Addressing the strategic approach that was being undertaken, Pain suggested Russia had initiated a deliberate strategy to "reprogram the mass consciousness" by promulgating new psycho-perceptual models of the world, to include a "new [type of] war" model, and a "Free Chechen" model, in which the Chechen people eagerly sought Russian liberation.[36]

By 2003, Russian military theorist S. P. Rastorguyev offered a description of information-centric conflict in which the final objective was to effect the knowledge of a specific information system (in context, clearly meant to include both machines and persons,) and the purposeful use of that knowledge to *"distort the model of the victim's world."* Clarifying that both target and means could be other-than-digital, Rastorguyev defined an information weapon as *"…any technical, biological, or social means or system that is used for the purposeful production, processing, transmitting, presenting, or blocking of data and or processes that work with the data."*[37] The same year, writing in Russia's Military Thought, S.A. Bogdanov suggested the goals of contemporary armed struggle were obtainable by a combination of "military, economic, and 'information-technical' and 'information-psychological' means,[38] suggesting the potential for Russian integration of Netwar with Cyberwar and traditional conflict. Thus, in Netwar per Bogdanov, one would expect to see the use of military power as a means to shape perceptions of a target audience (either in concert with, or absent traditional acts of violence); use of economic levers; and use of mass-media a-la *Information Psychologica*l, all integrated under a coherent strategy. A lesser, mere execution of *Information Psychological* alone, would at a minimum seek to engage mass media in the struggle, and seek to use it to distort target perceptions to Russian advantage.

However, Moscow faced difficulty in transforming these concepts into tools that worked reliably outside Russia. Writing in *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture, and Money*, authors Pomerantsev and Weiss suggest that when Russian authorities attempted to ensure victory for Viktor Yanukovych, a pro-Russian candidate in the 2004 Ukrainian elections, they found themselves unable to dominate the perceptual environment. As a result, at least one Russian media operative was forced to flee Ukraine in disguise as the Orange Revolution brought Victor Yuschenko to power. And four years later, during Russia's conflict with Georgia, despite securing services of external public relations firms and establishing the Russia Today (RT) television channel, Russian elites still perceived a failure to achieve victory in the external information domain.[39]

Perhaps in response to this weakness, structures Russia used to manage Netwar were once again revised. A position for a Presidential Special Advisor for Information and Propaganda Activities was established, and conduits under state control were expanded to include international "Non"-Governmental Organizations working alongside the Russian information

35 "Biography of Emil Pain" (Stanford University) accessed 5 December 2014 at http://web.stanford.edu/group/Russia20/pain_bio.htm..

36 Timothy Thomas, *supra* note 28 at 185.

37 S. P. Rastorguyev in *Id*. at 78.

38 S. A. Bogdanov, "The Probable Appearance of Future Warfare," (Voyennaya Mysl [Military Thought], 15 December 2003) as translated and downloaded from the FBIS website in May 2005, in *Id*. at 79.

39 Peter Pomerantsev and Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, New York, Institute of Modern Russia, 2014, 12.

agencies and "information troops made up of state and military news media"[40] By 2010, Rear Admiral Pirumov was already anticipating Gerasimov's more recent assertion that "wars are no longer declared and, having begun, proceed according to an unfamiliar template,"[41] describing information 'warfare' as an activity that would be conducted in *both wartime and peacetime*, with a goal of securing "national policy objectives" through exerting influence on an opponent's information systems and "psychic conditions"; via promulgation of disinformation; societal and situational manipulation; "crises control"; propaganda efforts directed at effecting "conversion, separation, demoralization, desertion, [and] captivity"; lobbying; and blackmail.[42] President Putin himself reinforced this conceptualization of an eternal battle of influence when he described "soft power" as consisting of a "matrix of tools and methods to reach foreign policy goals … by exerting information and other levers of influence."[43] [44]

At present, many believe this type of *Information Psychological* is being actively practiced by Russia. Michael John Williams, an Associate Scholar at the Center for European Policy Analysis, citing Gerasimov, Bogdanov, and Russian strategist Sergey Chekinov, describes something much like *Information Psychological* as the first of two phases in modern Russian conflict, suggesting that in phase one "…unconventional operations are undertaken to manipulate public opinion at home, in the target country and foreign press. Eventually Russian forces, under the guise of domestic militants, will be deployed. This marks the end of the unconventional operations. If successful, the Kremlin then uses legal language to legitimate the intervention as one protecting "human rights" in the target country. The second phase is thus a much more conventional operation. In the case of Crimea, the operation was so successful that the conventional deployment barely required a shot to be fired."[45] Canada's Foreign Minister Baird summarized the situation more succinctly, and with a focus on aspects of *Information Psychological* directed farther abroad, suggesting Russia was "…polluting the opinion-making process in the west…[via]…the active manipulation of information."[46]

Russia's Netwar tools are diverse: RT has expanded to include multilingual news, a wire service, radio channels, and enjoys a budget measured in the hundreds of millions of dollars.[47] "Voice of Russia" has re-branded itself as "Sputnik," and is establishing a network of media hubs in 30 cities abroad,[48] echoing the establishment of the media centers during the Chechen conflict. Some researchers suggest Moscow also employs armies of online "trolls" to supplement these overt channels, using multiple social media accounts to participate in online discussions, and recruiting thousands of Twitter followers under multiple online identities.[49] The existence

40 *Id*. at 12 and citing Igor Panarin in Timothy Thomas, RECASTING THE RED STAR, Foreign Military Studies Office, 2011.

41 Valery Gerasimov, *supra* note 26.

42 V.S. Pirumov, Informatsionne Protivoborstvo. Moscow, 2010, 3 quoted in Timothy Thomas *supra* note 39 and Peter Pomerantsev and Michael Weiss, *supra* note 39 at 12.

43 Putin's concept of "soft power," which closely approximates Netwar, stands in contrast to western views of "soft power" as a normative attraction derived from actions making one desirable as a model or ally.

44 Peter Pomerantsev and Michael Weiss, *supra* note 39, at 12.

45 Michael John Williams, *Russia's New Doctrine: How the Kremlin Has Learned to Fight Tomorrow's War Today*, Center for European Policy Analysis, 09 May 2014, accessed at http://cepa.org/content/russia%E2%80%99s-new-doctrine-how-kremlin-has-learned-fight-tomorrow%E2%80%99s-war-today.

46 John Baird, *Address by Minister Baird to the NATO Council of Canada Conference - Ukraine: The Future of International Norms*; 18 November 2014 - Ottawa, Ontario" accessed at http://www.international.gc.ca/media/aff/speeches-discours/2014/11/18b.aspx?lang=eng.

47 Peter Pomerantsev and Michael Weiss, *supra* note 39 at 12.

48 Stephen Ennis, *Russia's global media operation under the spotlight*, BBC NEWS ONLINE EUROPE, 16 November 2014, accessed at http://www.bbc.com/news/world-europe-30040363.

49 Peter Pomerantsev and Michael Weiss, *supra* note 39 at 17.

of such obscured meme amplification architectures may explain propagation of supposedly "leaked" satellite images purporting to show that Flight MH17 was downed by a Ukrainian aircraft, even as other online communities noted inconsistencies and brand the images fake.[50] However, arguments of "real" or "fake" may miss the underlying intent of *Information Psychological*. Pomerantsev and Weiss suggest Moscow *"...exploits the idea of freedom of information to inject disinformation into society ... not to persuade (as in classic public diplomacy) or earn credibility but to sow confusion via conspiracy theories and proliferate falsehoods [and] ... exacerbate divides."*[51] Fiona Hill, of the Brookings Institution is more direct, suggesting that *"Putin is aiming for that large swathe of the population, especially in the United States, that is non-conformist and deeply suspicious of their own government. Then in Europe there are those who follow populists on the far right and far left who are very prone to seeing their own governments as traitors to the national cause, or inept or overbearing."*[52] If these hypotheses are correct, the west should expect coordinated targeting of issues and communities pre-disposed to question domestic authority, and to accept – or at least entertain – alternate narratives that serve Moscow's interest. Information Psychological is thus not a logical contest, but an emotional contest for the hearts and minds of the swing votes and interests in targeted systems. And it is here that United Front Theory most clearly comes into play.

6. UNITED FRONT THEORY

"Cooperate with anybody who is not opposing us today, even though he did so only yesterday."[53] United Front Theory is, in simplest form, a strategy of a deliberately (and dynamically) shifting the boundary between ideological friend and foe in order to maximize the community aligned with a protagonist while isolating an opponent. Lyman Van Slyke, who chronicled the evolution of this approach within the Chinese Communist Party (CCP), suggests it emerged as a CCP tactic during the early 1920s,[54] [55] when CCP members (then a tiny minority) sought dual membership in the more powerful Nationalist Kuomintang (KMT) party as a means to initially reach, and ultimately co-opt, a greater number of followers.[56]

United Front Theory served as a useful tool to both guide and rationalize CCP policy regarding relations with, and accommodation to, the KMT. Toward the end of World War Two, Mao Tse-Tung suggested that in areas controlled by the KMT, Chinese communists should engage an extant social movement "…embracing various social strata…" and "…cooperate with anybody who is not opposing us today."[57] Here we see a willingness to put aside past conflict to realize a shared aim, but we should not read into this any intent of Mao to reach lasting accommodation

50 Will Stewart and Amy Ziniak, *Were MH17 'satellite images' photoshopped? Report slams new surveillance pictures released by Russian state broadcaster as a 'shoddy fake'* MAIL ONLINE AND DAILY MAIL AUSTRALIA, 16 November 2014, accessed at http://www.dailymail.co.uk/news/article-2836245/Report-slams-new-surveillance-photos-released-Russian-state-broadcaster-MH17-shot-shoddy-fake.html.

51 Peter Pomerantsev and Michael Weiss, *supra* note 39.

52 Mark Franchetti, Toby Harnden and Michael Sheridan, *Kremlin Calling*, THE SUNDAY TIMES, 16 November 2014, accessed at http://www.thesundaytimes.co.uk/sto/news/focus/article1484299.ece.

53 Mao Tse-Tung, in Lyman Van Slyke, ENEMIES AND FRIENDS: THE UNITED FRONT IN CHINESE COMMUNIST HISTORY, Stanford University Press, 1967, 168

54 Introduced by Hendricus Sneevliet, a Dutch Comintern agent operating first in Indonesia, and then in China's Eastern coastal cities.

55 Lyman Van Slyke, *supra* note 53 at 15.

56 *Id*.

57 Mao Tse-Tung, in *Id* at 168.

with the KMT! Instead, recognizing the CCP was better served for the moment by "uniting" with the KMT against the Japanese, Mao and his comrades placed the CCP in a position from which it could survive and build capacity for a future day, while still reserving the option to re-draw the boundaries that separated friend and foe.

This was exactly what occurred in 1945 when, following Japan's surrender, the CCP re-drew a boundary which still (at least nominally) included the KMT as allies, but posited the nebulous presence of elements that sought to perpetuate a civil war within China as the new enemy, in the knowledge that the US (at the time, a power the CCP sought to co-opt or at least neutralize) feared just such a civil war. Within a few months, the line was shifted again, as goals of "peace" and "unity" rapidly morphed into calls for "an anti-feudal united front" (language that both conformed to the rejection of dynastic legitimacy that underpinned both KMT and CCP platforms, while also subtly playing to more radical Communist concepts,) then ultimately into the existential need for an "anti-Chiang [Kai Shek, the KMT leader] united front."[58] I believe this meme evolution suggests United Front Theory guided a deliberate CCP information strategy to:

1. Present the CCP in a favorable light to both extant allies and potentially undecided parties
2. Co-opt potential resources of an opponent by actively and selectively framing the debate
3. Define, isolate, and ultimately destroy legitimacy of a specific, manageable subset of opponents

In other words, United Front Theory served the CCP as a Netwar management tool, allowing identification of potential *conceptual boundaries* that could be promulgated to isolate a specific subset of an adversary, while simultaneously framing the public debate in terms that deterred the target's potential allies from associating with it.

United Front Theory is based upon Marxist dialectics and theories of "contradiction," and as refined by Mao, posits the presence of both a principle contradiction and many lesser contradictions at any given moment. The principle contradiction cannot be resolved without struggle, and is thus deemed to be an "antagonistic" contradiction. Many lesser, "non-antagonistic" contradictions also exist, but can be put on hold until the initial "antagonistic" contradiction is resolved, and any third parties with whom a "non-antagonistic" contradiction exists may be dynamically co-opted within the United Front to facilitate resolution of the "antagonistic" contradiction. However, upon resolution of the primary "antagonistic" contradiction, by definition a new "antagonistic" contradiction will evolve to take the primary place. Thus at all times there is a core protagonist group, a "wavering" middle that may split either way, and an existential foe who must be destroyed or transformed into a non-contradictory entity.[59]

The art of executing United Front Theory is to reduce to the absolute minimum the boundaries of the entity deemed to be in "antagonistic contradiction" (thus allowing the most concentrated and efficient application of resources against it,) to co-opt (or deter from participation) the broadest possible swath of the "wavering" middle (thereby eliminating them as an adversary resource, and possibly leveraging them as a supporting resource,) and to anticipate, and stand

58 *Id*. at 188-189.
59 *Id*. at 249-251.

ready to re-draw, the new boundaries of contradiction as the strategic environment evolves (an opponent may also be seeking to do the same, and the new psycho-structural features, once established, may require significant effort to erode.) Mao and the CCP historically executed this evolution in fast geopolitical time, sometimes acting within days. In a modern age of targeted political messaging,[60] online A-B testing (the presentation of unique versions of a message to different groups within a targeted online audience, in order to measure responses and optimize desired effect,)[61] and near-real-time semantic analysis,[62] [63] United Front Theory can operate at netspeed.

7. LEGAL WARFARE

At this point it is worth noting that while information and sentiment may move at netspeed, their lumbering, normative counterparts - policy and law – still do not, and in the space between these two worlds, China has developed another facet of Netwar, "Legal Warfare" (or what Major General Charles Dunlap, Jr. has called "Lawfare."[64]) The leading western scholar of Chinese Legal Warfare, Dr. Dean Cheng, suggests that Legal Warfare illustrates a broader Chinese effort to expand conflict beyond the military domain.[65] One of "three [non-traditional] warfares" articulated in doctrinal writings by the modern Chinese state,[66] conduct of Legal Warfare accelerated in December of 2003 when policy – specifically, revised Political Work Regulations of the Chinese People's Liberation Army – directed the General Political Department (GPD) of the PLA to undertake "three warfares" as part of its implementation of political work.[67]

Operating in synergistic concert with the other two "warfares," psychological warfare (defined as fairly standard 'will-eroding' activities,) and public opinion/media warfare (*"…a constant, ongoing activity, aimed at long-term influence of perceptions and attitudes [via domestic and foreign] news media…movies, television programs, and books,"*) the function of Legal Warfare is to inculcate *"…doubts among adversary and neutral military and civilian authorities, as well as the broader population, about the legality of adversary actions, thereby diminishing political will and support and potentially retarding military activity."*[68]

Here one can see the potential intersection between Legal Warfare, as a *component* of Chinese Netwar, and United Front Theory, as a guiding *framework* for Chinese Netwar. Taking the PLA/GPD as our protagonist, the "antagonistic contradiction" can be defined as an undesired legal,

60 Kate Kaye, *Post Election, Campaigns Try to Link Targeted Ads to Actual Votes - Here's How Political Groups Know When Digital Ads Drove Voters to the Polls*, AdAge, 24 November, 2014, accessed at http://adage.com/article/datadriven-marketing/political-campaigns-link-voter-aimed-ads-actual-votes/295936/.

61 Brian Christian, *The A/B Test: Inside the Technology That's Changing the Rules of Business*, WIRED online, 25 April 2012, accessed at http://www.wired.com/2012/04/ff_abtesting/.

62 Seth Grimes, *What are the most powerful open-source sentiment-analysis tools?* 8 January 2012, Breakthrough Analysis, accessed at http://breakthroughanalysis.com/2012/01/08/what-are-the-most-powerful-open-source-sentiment-analysis-tools/.

63 2014 Sentiment Analysis Symposium, accessed at http://sentimentsymposium.com/.

64 Major General Charles J. Dunlap, Jr., USAF, *Lawfare Today: A Perspective*, YALE JOURNAL OF INTERNATIONAL AFFAIRS, Winter 2008, 146.

65 Dean Cheng, *Winning Without Fighting: Chinese Public Opinion Warfare and the Need for a Robust American Response*, 26 November 2012, accessed at http://www.heritage.org/research/reports/2012/11/winning-without-fighting-chinese-public-opinion-warfare-and-the-need-for-a-robust-american-response.

66 *Id.*

67 *Id.*

68 *Id.*

normative, or military activity undertaken or advocated by an adversary; and the "wavering" middle ground can be seen as all those "adversary and neutral military and civilian authorities, as well as the broader population" that may be swayed. The PLA operational objective is thus the *effect* of reducing opponent "…political will and support and potentially retarding military activity,"[69] achieved via a synergistic execution of Legal Warfare, psychological warfare, and public opinion/media warfare.

Dunlap notes, "information technologies have … vastly increased the scope, velocity, and effectiveness of such [Lawfare] efforts,"[70] and one need only look to Chinese online press to find candidate examples of United Front Netwar addressing legal disputes. For example, in the 2012 Xinhua article titled *"China's blueprint means opportunities, not threats,"* Chinese state media simultaneously suggested opposition to China in the legal domain would bring economic ruin, stoked regional fear of western decline and abandonment, and deterred "internationalizing" of legal disputes, arguing that "cementing economic bonds within Asia remains key to the region's continuous growth, as the eurozone sovereign debt woes are far from over, with a fiscal cliff threatening a fragile recovery in the U.S. economy and protectionism on the rise globally. Internationalizing the South China Sea issue will not help resolve the disputes but can sabotage efforts to carry out friendly negotiations on the issue and hamper much-needed regional economic cooperation."[71]

At first glance this might seem an expedient response to anomalous regional and international conditions, but if Cheng is correct, Legal Warfare (and the Netwar conducted in support) is not viewed by the Chinese as an action to be initiated upon tensions or hostilities, nor, as Dunlap suggests, as part of pre-existent "confines of the law"[72] which a Judge Advocate General (JAG) Officer might help warfighters navigate, but rather a cause to be constantly advanced in parallel with other "phase zero" shaping activities, and represents part of "…*the foundation* … [that] *must be established during peacetime so as to create beneficial conditions and context for the military conflict and, in turn, precipitate an early end to a conflict on terms favorable to the PRC.*"[73]

This suggests both peacetime legal claims, and Chinese contention of foreign legal claims *during* peacetime, should be evaluated not only as expressions of Chinese national interest, but also as both *preparation of* a multidimensional Netwar battlespace, and as a form of Netwar itself. In short, any would-be challengers to Chinese ambition must expect sustained, pre-emptive campaigns to reframe normative, legal, and military issues in ways that paint them as dangerous outliers while embedding Chinese goals within constructs likely to be, or already, embraced by a majority of stakeholders. This is a strategy unlikely to be countered by reactive efforts (which cede to China, or any other Netwar opponent, the ability to set the very boundaries of the front.) Instead, sustained counter-strategies, and analytic entities capable of delivering a thorough analysis of the dynamic normative and psychological terrain that these strategies must operate within, are needed.

69 *Id.*
70 Major General Charles J. Dunlap, Jr., *supra* note 64 at 148.
71 China's blueprint means opportunities, not threats, Xinhua News 22 November 2012, accessed at http://news.xinhuanet.com/english/china/2012-11/22/c_131993006.htm.
72 Major General Charles J. Dunlap, Jr., supra note 64 at 151.
73 Dean Cheng, *supra* note 65.

8. A ROLE FOR CYBERDEFENSE ORGANIZATIONS IN NETWAR

"Perhaps the most important future battlefield for psychological warfare, though, is the Internet..."[74]

The principle strengths of free societies may make them inherently more vulnerable to the effects of Netwar. Open 'information borders,' vital to debate and commerce, provide thin protection against tailored deceptions veiled as gossip, market preference, opinion, or social interaction. Yet, *inherent* vulnerability need not equate to *actual* vulnerability. While free nations are rightly reluctant to control or censor any legally conducted expressions of belief, there is no reason they cannot convey findings regarding a foreign influence campaign, the dubious origins of a propagating meme, or objective facts – no matter how uncomfortable a position they paint an offending nation in - to their own population. In fact, given that in the modern age the vast majority of content in a Netwar will at some point transit the Internet, and given that the "networked technology" of that Internet has sovereignty associated with it, one might argue that a truly responsive democracy must be prepared to warn of, and if needed counter, a range of Netwar actions directed at it in a timely and transparent fashion, or else be deemed to have ceded a measure of sovereignty over its own cyberspace.

If this is the case, then the technology and skills of a Cyberdefense organization will have important roles to play. In the civil sector, Cyberdefense traditionally entails heightened, near-real-time situational awareness of internet activity; maintenance and control of backup communication and networking capabilities held in reserve; and established advisory and consulting relationships with subject matter experts and counterpart organizations across industry, academia, and government. All of these tools may be of utility in countering a Netwar campaign.

For example:

1. Cyberdefense organizations could be tasked to identify the emergence of Netwar-associated memes and actions in open online content. To guard against any potential misuse, warning activities could be transparent to the entire population served, and capabilities could remain under both the operational control and oversight of duly elected civilian officials.

2. Cyberdefense tools to characterize quantitative and qualitative shifts in network activity[75] could be called upon to reconstruct, track, and attribute Netwar-associated activities. A nation or alliance's citizens deserve to know if ten-thousand seemingly different online identities, all confirming the "fact" of an occurrence that their own leaders dispute, are in reality merely five persons operating under orders from a basement within an adversarial nation.

3. If and when Netwar is executed in combination with other forms of warfare – either Cyberwar, or kinetic war – Cyberdefense organizations may possess the capacity to counter certain Netwar actions with potentially existential

74 *Id.*

75 See for example the Internet Storm Center at www.sans.org , or Google's TRENDS feature at www.google.com.

consequences. Cyberdefense organizations should be prepared to use any out-of-band communication capabilities, reserve modes, international partnerships, or civil-military-industrial interfaces they possess to enable an authoritative and timely response by their civilian leadership within the information domain.

Moreover, Cyberwar and Netwar have become increasingly intertwined, and the impact of cyber actions can be either potentiated or mitigated by corresponding psychological and normative conditions. Thus, an effective Cyberdefense must also incorporate a set of informed Netwar responses.

9. CONCLUSION

Responding to modern Netwar need *not* require the initiation of a Cyberwar in response, nor a claim in the United Nations Security Council that the threshold of any type of conflict (other than the here-defined concept of Netwar) has been breached. President Putin may express the sentiment that the west is conspiring against Russia[76] without his paranoia constituting a *casus belli*. So too is Minister Baird free to draw attention to ongoing Russian manipulation of information. But the west should not become complicit in affording such different, and differently-intentioned, statements conceptual equality on a national, regional, or global, media stage, nor should western decision-makers cling to the hope that Netwar opponents will refrain from elevating their own voices at the expense of truth, either overtly or through a façade of intermediaries.

Fortunately, the antidote to Netwar poison is active transparency, a function democracies excel in. A United Front, as it were, of truth-seeking nations, soberly facing their opponents, willing to accept the airing of one's own imperfection for the sake of improvement, and committed to the norm that there is an objective reality that matters, presents a formidable challenge to the information-machinations of undemocratic or authoritarian regimes. There is no reason the west cannot accept the insights in these eastern perspectives, and we should apply them, leveraging both new mechanisms and extant Cyberdefense organizations, within a morally appropriate Netwar framework, to advance our shared interests on the global stage.

76 Mark Franchetti, Toby Harnden and Michael Sheridan, *supra* note 52.