Irregular Warfare with Cyber Means

H. Kendircioğlu, T. Kaymazlı, A.A. Eker

***Abstract*—Conventional Warfare tries to defeat the enemy's military and coerces the opponent government to come to terms with. On the other hand Irregular Warfare concentrates on the population and tries to gain popular support and erode the opponent's legitimacy over people. Irregular adversaries are embedded in society and their easy access to communication and information technologies let them reach and organize people regionally and globally. Cyberspace presents lots of perfect tools to irregular warriors in the irregular battlefield.**

***Index Terms*— Irregular Warfare, Cyber Warfare, Cyberspace, Social Media, Social Networks.**

I. Introduction

THE collapse of the Soviet Union ended the Cold War era. CIA Director James Woolsey described the post-Cold War environment during his confirmation hearing in 1993 by saying "We have slain a large dragon (the USSR). But we now live in a jungle filled with a bewildering variety of poisonous snakes. In many ways, the dragon was easier to keep track of [1]." The end of the cold war was the beginning of new economic, social, and military challenges including ethnic conflicts, terrorism, and irregular warfare crises. While trying to get used to new irregular security environment, we faced another dimension of warfare; cyberspace. Cyberspace offers lots of tools for irregular actors to fight against states. Cyber warriors can target critical infrastructures to erode popular support and will of population to continue the war. Information and communication networks can be used to win the "battle of narratives", "war of ideas" and helps winning "hearts and minds" in the long run. Cyber capabilities, particularly the use of internet and social media enable "self organized civilians" to resist against states. It becomes harder for states to differentiate between combatants and non combatants causing collateral damage and arousing international interest over the conflict.

II. Irregular Warfare

Irregular Warfare is defined as; "a violent struggle among state and non-state actors for legitimacy and influence over the relevant populations. Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capabilities, in order to erode an adversary's power, influence, and will [2]." Irregular Warfare (IW) is not a new type of warfare. It is both a reality of our past and will be an indispensible part of our future. Although it is used to define the post cold war security environment, 9/11 terrorist attacks let the world realize the real scope and effects of the threat facing the world. As long as there are weaker and stronger parts of a conflict we will witness IW. Militarily weaker opponents will resort to irregular tactics to gain popular support and compensate the power gap between their enemies [3]. IW is thought to consist of guerrilla warfare, terrorism, sabotage, subversion, criminal activities, and insurgency [4].

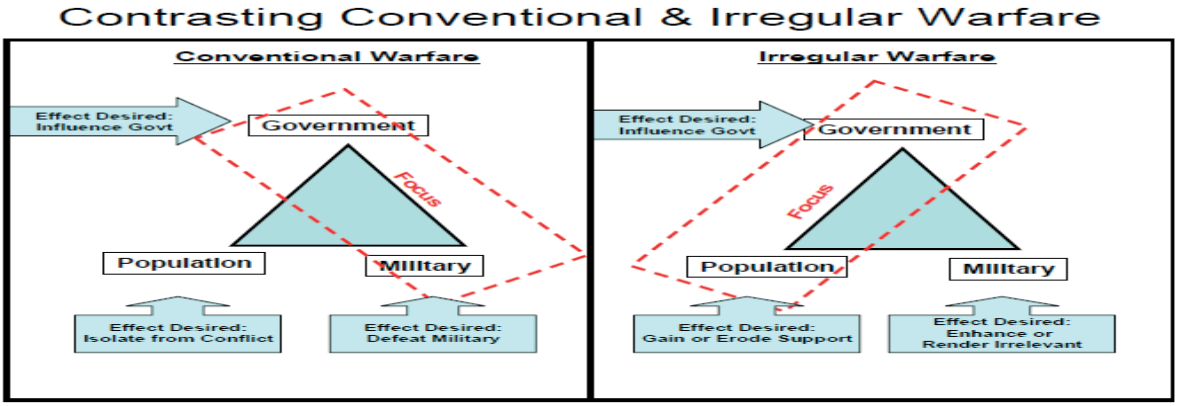

Fig. 1. Contrasting Conventional and Irregular Warfare [5].

H. K. War Colleges Command, Army War College, Student Officer, Yenilevent, İSTANBUL 34330 TURKEY (Pbx: +90 212 398-0100/3504, İstanbul-Turkey, e-mail: hkendircioğlu@yahoo.com)
T. K. War Colleges Command, Army War College, Instructor, Yenilevent, İSTANBUL 34330 TURKEY (Pbx: +90 212 398-0100/3504, İstanbul-Turkey, e-mail: tuncaykaymazlı@gmail.com)
A. A. E. War Colleges Command, Army War College, Instructor, Yenilevent, İSTANBUL 34330 TURKEY (Pbx: +90 212 398-0100/3504, İstanbul-Turkey, e-mail: alpereker99@gmail.com)

IW is a struggle directly related with the influence and legitimacy over population. As explained in the figure below, conventional warfare aims the destruction of the enemy militarily and then coerces the adversary government come to terms with. On the contrary, IW focuses on the population and tries to weaken the government's legitimacy over population by gaining or eroding support. In IW threats

posed by adaptive opponents such as terrorists, criminal networks and insurgents as well as states cannot merely countered by military means alone [6]. Threats are intermingled with population and "increasingly networked, adaptable and empowered by cyberspace to find new ways to recruit, collect intelligence, train, distribute propaganda, finance and operate [7]."

To deal with IW threats there are several mutually inclusive spheres which are "all facets of the same form of warfare" [8] as;

- Counterterrorism (CT),
- Unconventional Warfare (UW),
- Foreign Internal Defense (FID),
- Counterinsurgency (COIN),
- Stability Operations,
- Peace Keeping,
- Security Force Assistance (SFA),

Dealing with IW threats requires a "whole-of-government" approach. The two trends of 21st century; growing insurgencies, terrorism and growing use of web make it more complicated for military to cope with. As it is clarified in the table below, irregular actors are directed locally, logistically independent, ad hoc forces. They are self-organized civilians who come together for raids and skirmishes and then merge into community and continue their routine daily life.

TABLE I
CONTRASTING DIMENSIONS OF WAR**[9].**

Contrasting Dimensions of War	
Modern	**Irregular**
Organized	Informal
Advanced technology	At-hand technology
Logistics-dependent	Logistics-independent
National direction	Local direction
Coherent doctrine	Ad hoc doctrine
Decisive battle	Raids and skirmishes
Soldier	Warrior
Allies	Accomplices
Segregation	Integration

III. CYBERSPACE AND CYBER WARFARE IN THE NEW SECURITY ENVIRONMENT

Human kind have been living in four physical domains; land, sea, air, and space, and now we how the fifth one cyberspace. How cyberspace and cyber warfare effect IW? In order to answer this question first we have to define cyberspace and cyber warfare. Policy makers recognized the importance of cyberspace and cyber warfare with the cyber attacks on some countries' network systems in 2007 and 2008 [10]. But it is still impossible to draw the borders of cyberspace and cyber warfare. Cyber is a new phenomenon that no one knows where it begins and where it ends. It is a multidimensional dynamic stuff connected with lots of domains, and has many diverse characteristics that suggest that its future may differ significantly from its present [11]. The term "cyberspace" is used by William Gibson in his science fiction novel "*Neuromancer*" and took its place in our lexicon for two decades. Even so there is no consensus over the meaning of it. To give a comprehensive definition, Cyberspace is "*a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies* [12]."

It is possible to say that cyberspace and cyber warfare mainly take place through interconnected and interdependent information and communication technologies. Both of information and communication technologies are extremely used by IW actors such as, insurgents, terrorist organizations, multinational criminals and states.

In cyber warfare, preemptive strikes are favored. Well-trained cyber soldiers make it hard for any government to track down the origin of the attack and retaliate. As we mentioned before irregular warfare is about the legitimacy and popular support. The most critical impact of the cyber-attacks will be on the will of the population. Cyber weapons can be used to cause a cascading series of technology failures, beginning with the telecommunication systems, DDoS attacks against government sites, banking systems, and civil corporation networks. Cyber warriors target military technologies and critical civilian infrastructures, or anything else the adversary values, to create a chronic loss of services, such as, transportation system, causing mess in the airports, harbors, railways, damaging water pipeline, oil and nuclear power plants, electricity, overloading emergency calls, hospitals, releasing water from dams and causing flood, cutting media and communication channels, television, telephone services to name few. If attacks continue for weeks either in a continuous or sporadic mode, may cause chaos and loss of confidence in the government's capability to secure daily life and erodes popular support.

Besides aforementioned capabilities, cyberspace presents perfect tools for irregular fighters. According to the "Social Movement Theory" organizational skills are one of the most essential elements for success of any social movement [13]. In order to organize people without a targetable leadership is a significant asset for irregular warriors. With the invent of at-hand technology devices such as, smart phones and tablet PC's, cyberspace and social media offered opportunity for irregular warriors to influence people with activities including internet, television, radio, cell phones and special applications to generate self organized civilians. After the appearance of the internet, as can be seen in the Arab Spring, the ability of IW actors to organize simple minded civilians around a mutual goal to participate in their plans has risen significantly [14]. An Egyptian blogger explains it as; "*Before this social revolution, everyone was very individual, very single, very isolated and oppressed in islands. But social media has created bridges, has created channels between individuals, between activists, between even ordinary men, to speak out, to know that there are other men who think like me. We can work together, we can*

make something together [15].*"*

Legitimacy is directly linked with the strategy of "winning hearts and minds", "battle of narratives" or "war of ideas" and winning this battle is more important than actual achievements on the military battlefield. Cyberspace, particularly internet and social media have become the main arena for these battle of narratives. Social networks "open new opportunities to recruit the essential public support, international as well as domestic, to military operations [16]." Wars of ideas "…help boost morale and generate material contribution and other support for the physical fighting [17]".

Irregular warfare is generally not a technology intensive activity. It is a human centric form of warfare. But most of the modern armies are equipped with cutting edge weapon systems and experiencing difficulties in adapting to new irregular security environment. While dealing with irregular threats these $ billion investments get useless or in some cases harmful for the grand strategy by inflicting unintended casualties on civilians. It is difficult to differentiate between combatants and non combatants in an irregular conflict because combatants are inherent parts of the society and manage to get innocent civilians involve in the conflict by information and communication technologies. These collateral damages arouse international interest in the conflict and help insurgents or terrorists convey their purposes, goals and ideology by using cyberspace assets, social media, and internet to gain popular support and question the legitimacy of the states.

On the other hand, contrary to the states' $ billion investments, irregular warriors can cultivate simple tactics and weapons like improvised explosive devices and overcome technological superiority in irregular warfare. They can easily access every bit of information about weapons and their vulnerabilities and spread it worldwide through internet.

IV. Conclusion

New security environment resembles "a jungle filled with a bewildering variety of poisonous snakes." Militarily weaker parts of any conflict will most probably resort to tactics such as guerrilla warfare, terrorism, sabotage, subversion, criminal activities, and insurgency.

Cyberspace is also a new phenomenon which took place in our lexicon almost for two decades. Although there is no consensus over the definition of cyberspace, there is no doubt that it will be one of the indispensible parts of our life in the future. Interdependent and interconnected networks and devices using information and communication technology, offers perfect tools for irregular actors to gain or erode popular support and question the legitimacy of the opponent. It helps winning hearts and minds in the long run.

To win an irregular conflict which is a prolonged and low-technology intensive conflict, states have to have highly trained, culturally educated, joint capacity and interagency efforts.

Acknowledgment

We thank to War Colleges Command, Army War College, Dept. of Combat Tactic staff officers for their valuable contributions.

References

[1] I. Berman, Reviewed by Samara Greenberg, "Retaking the Offensive Against Radical Islam", *inFocus*, Winter 2010, vol 4, number 4, (2010), July 22, 2011, pp.140. http://www.jewishpolicycenter.org/2147/winning-the-long-war accessed by July 05, 2013.

[2] US Department of Defense,*: Dictionary of Military and Associated Terms*, Joint Publication 1-02 (JP 1-02), 2007 http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf accessed July 08, 2013.

[3] R. B. Scaife, "The Regularity of Irregular Warfare", *Small Wars Journal Article*, October 16, 2012. http://smallwarsjournal.com/jrnl/art/the-regularity-of-irregular-warfare accessed, July 08, 2013.

[4] S. G. Jones, *The Future of Irregular Warfare*, RAND Corporation March 27, 2012. http://www.rand.org/content/dam/rand/pubs/testimonies/2012/RAND_CT374.pdf accessed July 08, 2013

[5] US Department of Defense, *Dictionary of Military and Associated Terms*, Joint Publication 1-02 (JP 1-02), 2007 http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf accessed July 08, 2013.

[6] R. B. Scaife, "The Regularity of Irregular Warfare", *Small Wars Journal Article*, October 16, 2012. http://smallwarsjournal.com/jrnl/art/the-regularity-of-irregular-warfare accessed, July 08, 2013.

[7] S. G. Jones, *The Future of Irregular Warfare*, RAND Corporation March 27, 2012. http://www.rand.org/content/dam/rand/pubs/testimonies/2012/RAND_CT374.pdf accessed July 08, 2013

[8] R. B. Scaife, "The Regularity of Irregular Warfare", *Small Wars Journal Article*, October 16 2012. http://smallwarsjournal.com/jrnl/art/the-regularity-of-irregular-warfare accessed, July 08, 2013.

[9] J. B. White, *Some Thoughts on Irregular Warfare; A Different Kind of Threat*, Defense Intelligence Agency, April 14, 2007. https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol39no5/pdf/v39i5a07p.pdf accessed July 09, 2013.

[10] S. Mansfield-Devine, Estonia: "What doesn't Kill You Makes You Stronger", *Network Security*, July 2012, pp.12-20 http://www.sciencedirect.com/science/article/pii/S135348581270065X accessed June 10, 2013

[11] F. D. Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework", *Cyberpower and National Security*, Center for Technology and National Security Policy, Potomac Books, 2009. pp.3-23

[12] D. T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem", *Cyberpower and National Security*, Center for Technology and National Security Policy, Potomac Books, 2009. pp.24-42

[13] C. Jenkins, "Resource Mobilization Theory and the Study of Social Movements", *Annual Review of Sociology*, vol 9, 1983. pp.527-553

[14] O. Fridman, *The Power of Social Media: Analyzing Challenges and Opportunities for the future Military Operations*, University of London, March 20, 2013. http://academia.edu/3622572/The_Power_of_Social_Media_Analyzing_Challenges_and_Opportunities_for_the_Future_Military_Operations accessed July 09, 2013

[15] Egptian blogger Hassan Mostafa, cited in "Streetbook….." http://www.technologyreview.com/featuredstory/425137/streetbook/ accessed, July 10, 2013.

[16] O. Fridman, *The Power of Social Media: Analyzing Challenges and Opportunities for the future Military Operations*, University of London, March 20, 2013. http://academia.edu/3622572/The_Power_of_Social_Media_Analyzing_Challenges_and_Opportunities_for_the_Future_Military_Operations , accessed July 09, 2013

[17] A. J. Echevarria, *Wars of Ideas and the War of Ideas*, Strategic Studies Institute US Army War College, 2008. p.3 http://www.strategicstudiesinstitute.army.mil/pdffiles/pub866.pdf accessed, July 08, 2013.

AUTHORS' PROFILE

Hilmi Kendircioğlu received the B.S. degree in System Engineering from Turkish Military Academy in 2003. He was accepted in the Naval Postgraduate School (NPS) in California, and received M.S. degree in Special Operations Defense Analysis in 2011. He currently continues his study at the Turkish Army War College. He is interested in international terrorism, terrorism financing, cultural awareness, special operations, irregular warfare, cyberspace and cyber warfare.

Tuncay Kaymazlı War Colleges Command, Army War College, Instructor, Yenilevent, İSTANBUL 34330 TURKEY (Pbx: +90 212 398-0100/3504, İstanbul-Turkey, e-mail: tuncaykaymazlı@gmail.com)

Alper Alpaslan Eker War Colleges Command, Army War College, Instructor, Yenilevent, İSTANBUL 34330 TURKEY (Pbx: +90 212 398-0100/3504, İstanbul-Turkey, e-mail: alpereker99@gmail.com)