12-3-2012

Exterminating the Cyber Flea: Irregular Warfare Lessons for Cyber Defence

Ben Whitham
University of New South Wales

DOI: 10.4225/75/57a845eebefb3
13th Australian Information Warfare and Security Conference, Novotel Langley Hotel, Perth, Western Australia, 3rd-5th December, 2012

EXTERMINATING THE CYBER FLEA: IRREGULAR WARFARE LESSONS FOR CYBER DEFENCE

Ben Whitham
University of New South Wales, Sydney, Australia
ben.whitham@student.adfa.edu.au

Abstract

Traditional approaches to tactical Computer Network Defence (CND), drawn from the lessons and doctrine of conventional warfare, are based on a team of deployed security professionals countering the adversary's cyber forces. The concept of the adversary in cyberspace does not fit neatly into the conventional military paradigms. Rather than fighting an identifiable foe, cyber adversaries are clandestine, indistinguishable from legitimate users or external services, operate across state boundaries, and from safe havens that provide sanctuary from prosecution. The defender also faces imbalances with rules of engagement and a severe disparity between the cost of delivering the defence and the attackers ability to deliver an effect. These operational conditions are more akin with Irregular Warfare (IW) than a conventional conflict.

This paper proposes a new approach to CND, based on a review of the literature on IW. Rather than fight the battle alone, the CND team should concentrate efforts to persuade and empower network users to take responsibility for protecting the organisation's critical data. This approach seeks to apply the lessons learnt from IW, where the resistance to the adoption of security best practices, intentional or otherwise, is the real adversary. This approach appears more likely to deliver long term protection from the current cyber threats than a process, which requires the identification and tracking of adversaries that are invisible and constantly changing.

Keywords

Irregular warfare, computer network defence, cyber-war, counter-insurgency, cyber-security

INTRODUCTION

"Analogically, the guerrilla fights the war of the flea, and his military enemy suffers the dog's disadvantages: too much to defend; too small, ubiquitous, and agile an enemy to come to grips with. If the war continues long enough … the dog succumbs to exhaustion and anaemia without ever having found anything on which to close its jaws or to rake with its claws." (Taber 2002)

Conventional or regular warfare is a form of conflict between states that employs direct military operations to defeat an adversary's armed forces, destroy an adversary's war-making capacity, or seize territory in order to compel a change in an adversary's government or policies (U.S. DoD, 2007). Irregular Warfare (IW) differs from conventional warfare by its emphasis on the indirect approach, avoiding a direct military confrontation (Mao 2001). Instead one party employs methods not sanctioned by international law or customs of war, such as guerrilla warfare, terrorism, sabotage, subversion, criminal activities, and insurgency to subvert and exhaust the opponent (U.S. DoD, 2010). IW replaces other terms previously used in U.S. doctrine, such as low-intensity conflict, (LIC) and Asymmetrical Warfare, Operations Other Than War (OOTW) and 4th Generation Warfare (U.S. DoD, 2006).

Sharp (1999) was first to suggest that "the open architecture of the Internet is ideally suited for asymmetrical warfare". Rattray and Healey (2011) recently recommended that the U.S. Department of Defense "should analyse the dynamics of, irregular cyber warfare, as a major aspect of the development of cyber war doctrine and operational concepts. This might drive internal procedures based on familiar concepts of irregular war, rather than the arcane and poorly understood jargon of computer security". Unfortunately Rattray and Healey didn't provide specifics. This research aims to address this.

This paper is organised into three sections: (1) a set of observations, from literature, on why the IW environment and that experienced by CND operators is similar, that supports the observation by Sharp, (2) a proposed new IW-like overarching approach to conducting CND, based on IW literature, and (3) a transferrable advice on the conduct of CND based on IW experience, as recommended by Rattray and Healey.

SIMILARITIES BETWEEN IW AND COMPUTER NETWORK DEFENCE (CND)

The Absence of a Front Line or Operational Boundary

IW presents no defined battleground, no vanguard, no walls, nor opposing forces fronts and flanks (Cassidy 2004). Absence of a front line means that there are no longer any safe rear areas and support echelons are as much of a target as combat units (Hoffman 2006). With the introduction of necessary external interactions and trust relationships through bring your own devices, mobile smart phones and cloud computing, critical information is at rest and in motion inside and outside the traditional network boundary (see Fig 1). CND approaches of treating the protection of a computer network like the defence of a hill is likely to become less relevant (only allowing access to those inside the network, building perimeter defences, monitoring gateway traffic and hiding critical servers behind locked doors).

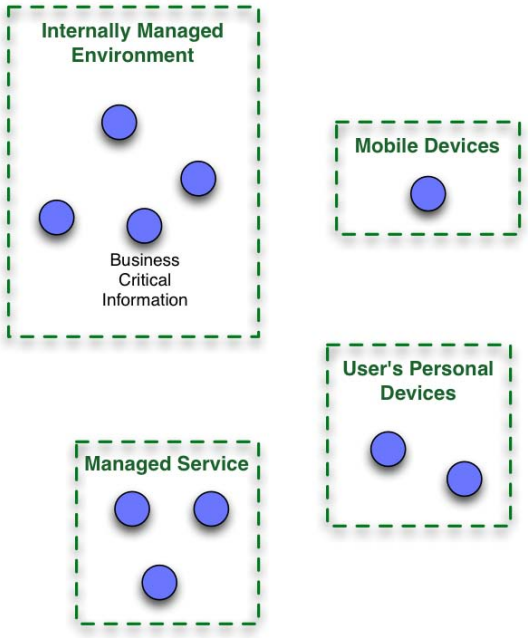

Figure 1: Critical data is no longer managed only within the internally managed environment

Constant Conflict with Uncertainty Between Friend and Foe

Modern land warfare, until recently, was divided up into three distinct phases: pre-conflict, conflict and post-conflict (Stockings, 2007). IW conflict rarely results in a single, rapid strike, and swift and victorious campaigns. Instead the distinction between states of war and peace in IW conflict collapse, as conflicts lasting months or years result in deadlocks, with neither side able to decisively conclude the conflict (Kiras 2008). What results is an uncertain environment where every individual citizen or issue motived group has the potential to become a friend or enemy, or both at different times during the course of the military engagement (Anderson 2011). Similarly, the Internet in its natural state contains both friendly and compromised hosts, and hostile and neutral users, where neither state is permanent, guaranteed or absolute.

Organisations fighting an IW conflict have no interest in wearing military uniforms or other distinctive signs (Parks, 2003) and disperse their forces into small, mobile combat teams to become invisible by blending in with the local population to avoid identification and detection (U.S. DoD, 2005). Similarly, the Internet's architecture makes the identity of, and the motivation for the intrusion extremely difficult to ascertain. A sophisticated attack can be made to appear indistinguishable from legitimate users or external services (J. Hunker, et al, 2008) Often, the perpetrators of such activities can only be inferred from the target based on circumstantial evidence (United Nations, 2010). This allows criminals, insiders and nation states conducting limited intervention or exploitation activities to hide their identity and intent from the defending force.

Adversaries with the ability to adopt new technology and strategies

IW adversaries appear to be increasingly adaptive and sophisticated, able to outpace state-based militaries in the dialectic and competitive learning cycle inherent to wars. Their size and structure allows them to adopt technology earlier than traditional military structures and capability development (Hoffman, 2006). Similarly, cyber criminals are able to exploit software vulnerabilities within hours of their public notification.

Predominance of Non-State Actors

Conventional military operations are generally conducted with an assumption that the indigenous populations within the operational area are non-belligerents (U.S. DoD, 2007). Non-states actors, such as cybercriminals and hackivists have adopted state-like cyber attack and exploitation capabilities; and have become the prevalent threat on the Internet. Their operations have grown increasingly sophisticated, combining open source and bespoke software that was once the realm nation-states. As a result, military defenders will need to plan to defeat cyber threats coming from a number of different non-state sources, simultaneous to any traditional military threats in there area of operations.

Rule of Engagement Disparity

IW conflict presents challenges when combatants conduct conflict from within third party non-combatant infrastructure or employ violence indiscriminately to achieve their goals. This is in direct contravention to The Hague Conventions of 18 October 1907 and the 1949 Geneva Conventions for the Protection of War Victims, which define rules to protect non-combatants from unnecessary suffering. Similarly cyber security defenders are bound by local and international laws, which their adversaries may not elect to observe, such as pivoting an attack through a series of third party network hosts, or attacking a neutral service provider that may be hosting military services, amongst other customer data, in order to achieve an effect. Defenders also have challenges with electronic evidence collection and jurisdictions that make prosecution difficult. In addition, existing tracing and offensive technologies that could deliver attribution or a response option (or the threat of deterrence) are quite likely in conflict with domestic and international law (Gaycken, 2010).

Disproportionate Cost Between the Intruders and Defenders

The cost of IW is not equitable between combatants. There is a disproportionate cost between an improvised explosive device and the costs of equipping an entire military force with additional vehicle and personnel armour as well as sophisticated electronic equipment to detect and neutralise remote wireless detonation. In early 2012, there were approximately 432,000 counterinsurgency forces in Afghanistan. In addition, the U.S. spent over $100 billion per year on the conflict. Conversely, the Taliban, deployed less than one tenth of the forces, and had annual revenues of $150 million (Jones, 2012).

CND operators require expertise in all of the systems and networking protocols employed by the military organisation. The attacker has the distinct advantage of being able to choose the time and place of the attack and only needs to be familiar with those components and protocols of the defender's network that are vital to the offensive operation. In addition, the "price" an adversary pays for a capability-a tool or weapon-can be slight; the cost and impact borne by the victim of his attack can be very high (Alexander, 2010).

CHALLENGES TO THE CURRENT CND APPROACH

Lack of Personnel

The traditional approach to CND focuses on the adversary, attempting to parry each cut and thrust as it was identified. It allocates the responsibility for the protection of the critical information to a team of detection and response specialists. An example of this approach is the Kill-Chains proposed by Hutchins, et al (2011).

This type of approach enables CND operators to identify patterns that link individual intrusions into broader campaigns, they: (1) require CND operators (a limited resource) to lead the activity, and (2) would grow in complexity requiring militaries to sink ever-increasing resources into the team protecting the data as the lack of definable boundaries, the uncertainty between friend and foe and the rate of change in technology become overwhelming.

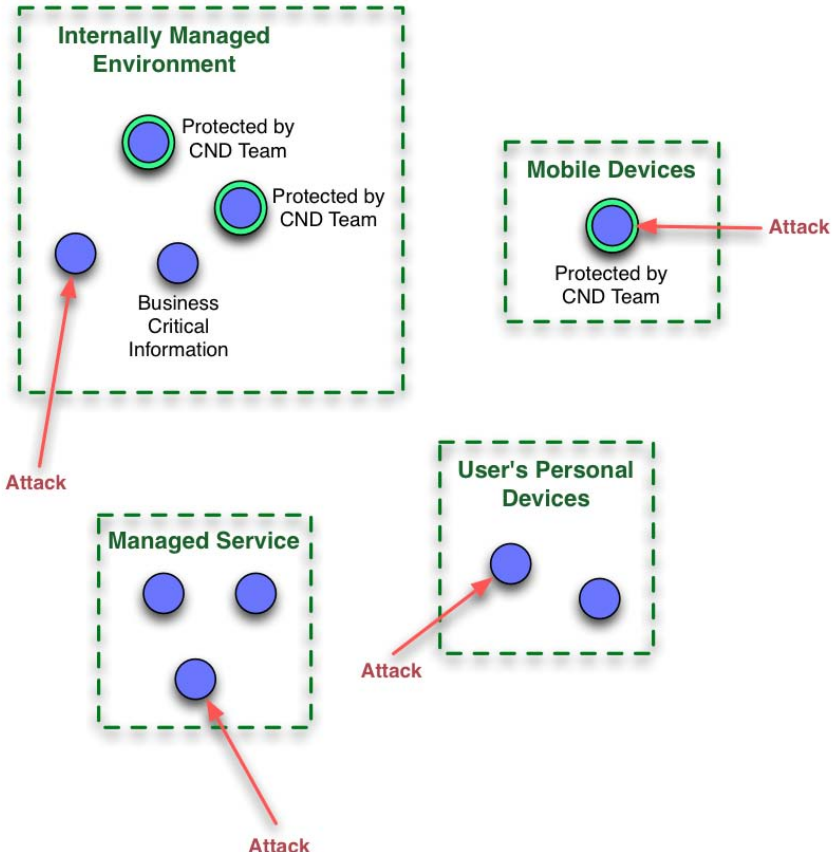

Figure 2: Conventional approaches to CND predominantly rely on the CND team to protect the critical information

Not Addressing the Highest Priorities

While developing Kill-Chains can help to detect adversary attacks, adopting best security practices can significantly reduce the risk of data loss to all cyber adversaries, regardless of origin or motivation. The Australian Defence Signals Directorate (DSD) advise that the adoption of the first four control measures in the Top 35 Mitigation Strategies would successfully counter 80% of the network intrusions that they have detected on government systems (DSD, 2011).

The adoption of security controls measures is not necessarily directly aligned with organisational outcomes. Adoption may result in restrictions on flexibility and/or ability to access, store and process data. They may reduce work productivity, which in a military context could mean a delay to the delivery of vital information to a tactical commander. For instance, DSD (2011) recommends that the most valuable two strategies to prevent targeted intruders are to patch operating systems and third party applications. The challenge is that undertaking this activity requires the system owners to: (1) accept a loss of service while the patch is applied, and (2) deploy the patch without sufficient testing, potentially risking additional service interruptions. This needs to be balanced with the security of the information on the network, the loss of which could impact the outcome of future military activities, or partner relationships, if confidence is lost. Based on DSD's research, making sure that tactical users are comfortable with constant network outages to apply necessary software patches, and the risk that there could be a further interruption due to an unlikely event of a software conflict as a result of rapid deployment of the patch and limited testing, is more likely to defeat both nation-state and cyber IW threats than building a team with skills in tactical network forensics.

A PROPOSED IW-LIKE APPROACH TO CND

The current U.S. Military IW definition is "a violent struggle among state and non-state actors for legitimacy and influence over a specific population" U.S. Department of Defense 2010). The proposed IW-like approach to CND considers the CND operator's own network users as the target "population" and the insurgency as the resistance to adopt best practices to protect data security. The IW-like approach to CND focuses CND operator effort on working directly with the network users to create an environment where network users are driving the adoption of security policies because they want to protect their data, dramatically increasing the size of the defenders protecting the network (see Fig 3).

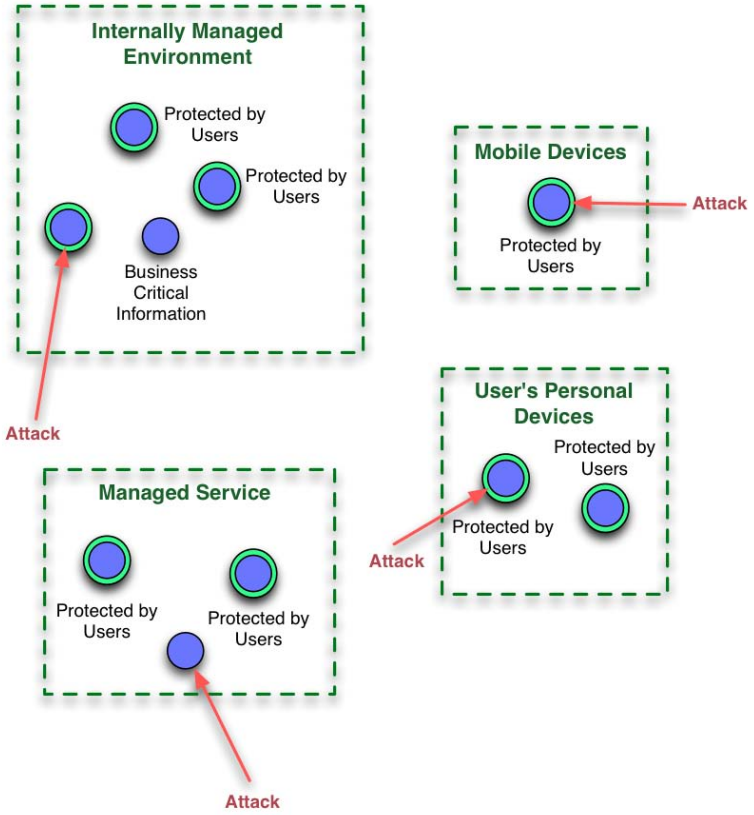

Figure 3: An IW-like approach to CND empowers the users and expands the number of people actively protecting the critical data

Resistance to the adoption of best practices could be as a result of apathy, indifference or a lack of understanding of the threat or impact of the users' activities (or lack thereof) on the organisation. The IW goal, therefore is to identify the source of the resistance and apply IW best practice to modify network user behaviour and attitudes.

APPLYING LESSONS FROM IRREGULAR WARFARE TO CND

Small steps

U.S. Field Manual (FM) 3-24, Counterinsurgency, recommends that IW forces do not "try to crack the hardest nut first - do not go straight for the main insurgent stronghold or try to take on villages that support insurgents." Instead, the manual recommends that IW forces "start from secure areas and work gradually outwards… Go with, not against, the grain of the local populace. First, win the confidence of a few villages, and then work with those with whom they trade, intermarry, or do business…achieving steady progress toward a set of reasonable

expectations may increase the populace's tolerance for the inevitable inconveniences entailed by on-going [IW] operations".

While the temptation could be to commence an organisation wide programme to address the results of an audit or penetration test, the initial engagement should start with supportive users and system owners. Success could allow for further measures to be applied with this same group, or, depending on the path of least resistance start an engagement in a new area using the introductions and support from the first.

User Empowerment

U.S. doctrine, FM 3-0, Operations, states that: "winning battles and engagements is important but alone is not sufficient. Shaping the civil situation is just as important to success." Kilcullen (2009) adds: "environment of cooperation needs to be developed, relying on a close and genuine partnership that puts the Host Nation forces in the lead". Ultimately the data on the network is from or for the user, and not as a direct result of the efforts of the IT security staff. Rather than adopting the control measure of highest priority first, allow the system owners to drive the pace and direction of the change. Working with the users to understand their priorities is more likely to yield success, and give the users a sense of ownership that can lead to self governance of data protection, as opposed to dictating the implementation from a prioritised list, based on a generic organisation-wide risk assessment. The latter only results in the continual requirement to invest in internal policing resources (compliance) and the growth of the resistance to further policies.

Live amongst the population

Jones (2012) states that: "The best way to win over the population and isolate the insurgents is to live among the population" This suggests that CND operators develop a clear appreciation of the activities that the users undertake and the conditions under which they operate. Too often the IT or IT security staff operate in isolation from the majority of the user community, without a clear understanding of the business of the organisation and when security policy is decreed across the organisation that impacts on the operational activities of users, it is understandably met with resistance and confusion.

Intelligence led operation

FM 3-24 states that: "IW is an intelligence-driven endeavour." The manual recommends the employment of standard intelligence processes to understand the operational environment, with emphasis on the populace, host nation, and insurgents in order to best address the issues driving the insurgency.

As per a traditional adversary-focussed CND approach, there is a requirement to monitor and understand the threat actor's capabilities. However, in addition, the IW approach also develops an understanding of the internal organisation. Assessments should be made to identify pockets or resistance, the extent of the resistance to change, the basis for why controls cannot be adopted, and "safe havens" or enclaves within the organisation that operate independent to the enterprise environment. In industry terms this could be specialist IT systems that have been delivered as a trial or have their own autonomy.

Response force supported by long-term reconstruction resources

Galula (2006) outlines a seven-step process for counterinsurgents. The first two stages are: expel insurgents followed by emplacing static forces. The static forces are provided to work with the community to ensure that it is able to start to return to normalcy and eventually, take responsibility for its own protection. The latter is not something that is not usually immediately achievable, but requires a long-term commitment from the IW force.

When a cyber security incident occurs, it is important to not only deploy the response capability, but also allocate sufficient resources to remain engaged with the impacted users over a sustained period of time. This requires a CND force balance comprising of an incident response team that is continually reactive to incidents supported by a much larger team that has the ability to work with the system owner to address the root cause of the incident and minimise the risk of a reoccurrence. The long-term support team needs to be capable of addressing policy and procedural short falls as well as capable of project managing the delivery of technical controls measures, such as installation of additional hardware and software or the migration of data. Like IW operations, this support team needs to have the ability to engage the users in a language that the users are able to understand; liaison and project management skills may not necessarily be the focus of conventional CND training.

Irwin (2009) recommends that the best leaders should be chosen to conduct a direct and long-term engagement activities, as they are likely to have the greater impact on the long-term strategy of compliance and self-support, rather than the response force. This strategy differs from traditional approaches where more capable staff may have been allocated to the higher profile incident response team.

Faster pace of adoption and greater agility

A recurrent theme throughout IW literature is the side that learns faster and adapts more rapidly - the better learning organisation usually wins (Nagl 2005, Luttwak 2006 and U.S. DoD 2007). Cyber security is constantly in a state of change. Software vulnerabilities are continually identified and computer networks are typically forever in a state of re-engineering and flux. Maintaining pace with technological, as well as procedural changes requires the willingness and the organisational structure to undertake continual improvement.

CND teams need to include sufficient resources to monitor IW requirements, such as changes in the organisation, the network and the operational environment as well as traditional CND adversary focussed intelligence and research. Cost effective delivery of general open-source intelligence can be provided through subscription to existing civilian authorities. Similarly, tactical CND operators can leverage off strategic agencies for more military specific content. Adoption of new technologies also requires the ability to learn and apply within a tactical environment. Time to undertake this activity, in addition to normal combat operations can be challenging, but is essential to ensure that best practices are adopted.

Offensive action

The combination of offensive and defensive actions is integral to the success of IW (U.S. DoD 2005). Offensive action in CND IW terms refers to the delivery of more active measures to encourage support of efforts to empower the users to secure their data. Offensive actions could include the delivery / production of awareness programmes, user training, penetration testing, compliance audits, threat assessments, active demonstrations, incident summary reports and CND intelligence reports. Offensive actions should be considered for areas or individuals that continue to resist the adoption of best security practices, or impact on the ability of existing agreed programmes, without reasonable cause.

FM 3-24 states that where possible small measured actions should be undertaken, rather than large-scale campaigns; “sometimes, the more force that is used, the less effective it is”. Ultimately the aim is to raise awareness of the threats in a manner that fosters a desire to protect critical data, without the need for continual coercion. The key, as it is with IW, is to know when more effort is required, and when it might be counter productive. Over exuberance without consideration for the operational considerations could result in a loss of credibility, which could create even greater resistance to the current proposals and present barriers for the adoption of future changes.

CONCLUSION

“The American military culture regarded Vietnam as an aberration, or, an exotic interlude between the wars that really count. The Army simply performed its conventional warfare repertoire in Vietnam even though it was frequently irrelevant to the situation” (Jenkins, 1970).

Defence personnel are much more likely to understand their role in cyber conflict if they are told to build cyber walls and conduct cyber patrols of their environment looking for their natural adversary (Nye 2011). The challenge for militaries is that the cyber environment does not have defined areas of operation and front lines, nor does it have defined nation-state actors. This paper proposes an IW-like approach to the challenges of CND, based on an idea proposed by Rattray and Healey (2011). The proposed IW-like approach to CND considers the CND operator’s own network users as the target “population” and the insurgency as the resistance to adopt best practices to protect data security, whether that be institutional, intentional or as a result of a misunderstanding. The IW-like approach to CND focuses CND operator effort on working directly with the network users to create an environment where network users are driving the adoption of security policies because they want to protect their data. Useful lessons from IW include: (1) addressing supportive areas first and grow support for the adoption of policy, rather than focus on areas of the organisation that might have the greatest need, (2) allow the network users to drive the pace of the change, (3) create a separate team that works with the users after an incident to hep them address the policy or technical root cause, (4) allocate a greater level of CND training effort to project management and interpersonal skills, (5) appoint the most talented CND staff to undertake the outreach and remediation programmes, rather than incident response, (6) resource agility, and (7) monitor, and where required, take action on areas that resist the adoption of key reforms.

REFERENCES

Alexander, Keith B. (2010). *Statements by Commander, United States Cyber Command, Before the House of Representatives Committee on Armed Services*, 23 September 2010, available at: < http://armedservices.house.gov/pdfs/FC092310/ AlexanderStatement.pdf > Accessed 4 October 2010.

Anderson, Ben. (2011). *Facing the Future Enemy* in Theory, Culture & Society, vol 28, no 7-8, pp 216-240.

Brady, Michael J, (1990). *The Army and the Strategic Military Legacy of Vietnam*. Master's Thesis. U.S.Army Command and General Staff College}

Galula, David (2006). *Counterinsurgency Warfare: Theory and Practice*. Greenwood Publishing Group.

Gaycken, Dr. Sandro (2010). *"The Necessity of (Some) Certainty--A Critical Remark Concerning Matthew Sklerov's Concept of 'Active Defense'", Journal of Military and Strategic Studies, Vol.. 12, Issue 2, Winter.*

Frank G. Hoffman. (2006). *Complex Irregular Warfare: The Next Revolution in Military Affairs*. Elsevier. Summer. p 395-411 Orbis. Irregular Warfare

Hunker, J. Hutchinson, R. and Marguiles J. (2008). "*Critical Information Protection II*", International Federation for Information Processing, Volume 290, eds. Papa, M., Shenoi. S., Boston: Springer, pp 87-99.

Hutchins, Eric. M. Cloppert, Michael. J., and Amin, Rohan. M. (2011). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Lockheed Martin Corporation Whitepaper. Lockheed Martin Corporation. In Proc. of ICIW 2011, pp. 113-125, Academic Conferences International, Mar 17th.

Jenkins, Brian. M., (1970). *The Unchangeable War*. RM-6278-2-ARPA. Santa Monica, CA: RAND.

Jones. Seth. G. (2012). *The Future of Irregular Warfare* Before the Committee on Armed Services Subcommittee on Emerging Threats and Capabilities United States House of Representatives, March 27. The RAND Corporation

Kilcullen, David. (2009). *The Accidental Guerilla: Fighting Small Wars in the Midst of a Big One* (New York: oxford University Press USA.

Kiras, James. D. (2008). *Irregular Warfare* in Understanding Modern Warfare, Cambridge University Press, Cambridge.

Luttwak, Edward. N. (1983). "*Notes on Low-Intensity Warfare*," Parameters XIII, no. 4.

Mao Zedong. (2001). *On Guerilla Warfare*, trans Samuel B. Griffith. Urbana, IL, University of Illinois Press

Nagl, John. A. (2005). *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya to Vietnam* (Chicago: University of Chicago Press.

Nye, Jr. Joseph S. (2011). *The Threat from Power and National Security in Cyberspace* in America's Cyber Future: Security and Prosperity in the Information Age Eds Kristin M. Lord and Travis Sharp June 2011. Center for New American Security. Washington DC.

Parks, Hays. (2003). *Special forces, Wear of Non-Standard Uniforms*, Chicago Journal of International Law, Vol. 4, No. 3, 2003, pp. 524-539 and 547-560.

Rattray, Gregory. J. and Healey, J. (2011). *Non-State Actors and Cyber Conflict in America's Cyber Future: Security and Prosperity* in the Information Age, Eds Kristin M. Lord and Travis Sharp, Center for New American Security. Washington DC.

Sharp, Walter. Gary. Sr. (1999). "*Redefining National Security in Today's World of Information Technology and Emergent Threats*", in Duke Journal of Comp. & Int. Law.

Stockings, C. (2009). *The Domain in which we Dwell: The Foundations, Form and Future of Land Warfare*, Strategic & Defence Studies Centre, Australian National University, Canberra, Working Paper Number 403, April, 2007.

Taber, R. (2002). *War of the Flea: The Classic Study of Guerrilla Warfare*, Brassey's.

United Nations. (2010). A/65/201, 30 July 2010, *Report of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, available at: < http://www.unidir.org/ pdf/activites/pdf5-act483.pdf> Accessed 4 October 2010}.

U.S. Department of Defense. (2010). *Irregular Warfare: Countering Irregular Threats*. Washington, DC: U.S. Department of Defense.

U.S. Department of Defense. (2006). *Irregular Warfare Special Study*. Joint Warfighting Center. USJFCOM Suffolk, Virginia.

USSOCOM and USMC. (2007). *Irregular Warfare Joint Operational Concept (JOC),* Version 1.0. Washington, D.C.: U.S. Department of Defense

U.S. Department of Defense. (2005). *FM 3-0 Operations*. Washington, DC: U.S. Department of Defense.

U.S. Department of Defnese. (2007). *FM 3-24, Counterinsurgency*, Headquarters, Department of the Army.

Weigley, Russell. F. (1984). *Reflections on Lessons from Vietnam. In Vietnam as History*. ed. Peter Braestrup. Washington, DC: University Press of America,.