

Maskirovka In The Information Age

by LTA(NS) Chin Hui Han

Abstract:

The author examines the power of deception in the context of information operations in the modern hybrid battlespace. Examples discussed include the Normandy landings in World War Two (WWII) and the use of the Russian Maskirovka doctrine in the ongoing conflict in the Donbass regions. The author then discusses the information space as the new battlefield in which dominance is highly prized by the modern war-fighter. He adds that a democratic platform, with avenues for influence and exploitation by all parties, civilian or military, is a quagmire in which militaries globally have had to adapt operations and technologies to conduct information operations to increase situational awareness. Lastly, the author then examines the efforts in information operations that the Singapore Armed Forces (SAF) has undertaken today as part of the 3rd Generation transformation.

Keywords: Information; Advantageous; Deceive; Cognisant; Vigilant

"All warfare is based on deception"

- Sun Tzu¹

INTRODUCTION

Russia's annexation of Crimea on 21st March, 2014 caught almost everyone off guard. The Russian military categorically disguised its actions and vehemently denied them but the 'little green men' who popped up in the Black Sea peninsula were a textbook case of the Russian practice of military deception or 'Maskirovka'.² Given the common belief that the Western Powers had every meter of the world monitored by reconnaissance satellites and every electronic information channel tapped, a theory further perpetuated by increasingly recurrent leaks of classified information, this was a particularly astounding feat.³ We live in times where it is taken for certain that there exists no means by

which a large military operation can be undertaken without triggering one of many alerts—but the annexation of Crimea has shown that the place of the supposedly-antiquated military strategy of deception lies very much in the modern information age.

Deception exploits the efficacy of surprise to achieve military goals by concealing or disguising intentions and the operational details of one's forces. The ability to manipulate and disseminate information today has greatly amplified deception capabilities and expanded its influence beyond strategic domains to the tactical levels.

This essay examines the power of deception in the context of information operations in the modern hybrid battlespace. We will study the use of deception in the Normandy landings in World War Two (WWII), the mitigation of air superiority by the

Serbians in the Kosovo War and the use of the Russian Maskirovka doctrine in the ongoing conflict in the Donbass regions.

Deception exploits the efficacy of surprise to achieve military goals by concealing or disguising intentions and the operational details of one's forces.

This is followed by a discussion of the information space as the new battlefield, in which dominance is highly prized by the modern war-fighter. The media landscape that forms the backdrop of these campaigns however, proves as neutral a fighting ground as the physical terrain. A democratic platform, with avenues for influence and exploitation by all parties, civilian or military, is a quagmire in which militaries globally have had to adapt operations and technologies to conduct information operations to increase situational awareness.

Lastly, the essay will examine the efforts in information operations that the Singapore Armed Forces (SAF) has undertaken today as part of the 3rd Generation (3rd Gen) transformation. We will make suggestions for the future SAF to expand its information operations to counter future deceptive threats, with a vision of elevating information operations from its role of a supporting character to a key player in mission planning and execution. This will pave the way for the efficient detection of deception, and the employment of counter-deception measures in a dynamic battlespace.

THE POWER OF DECEPTION

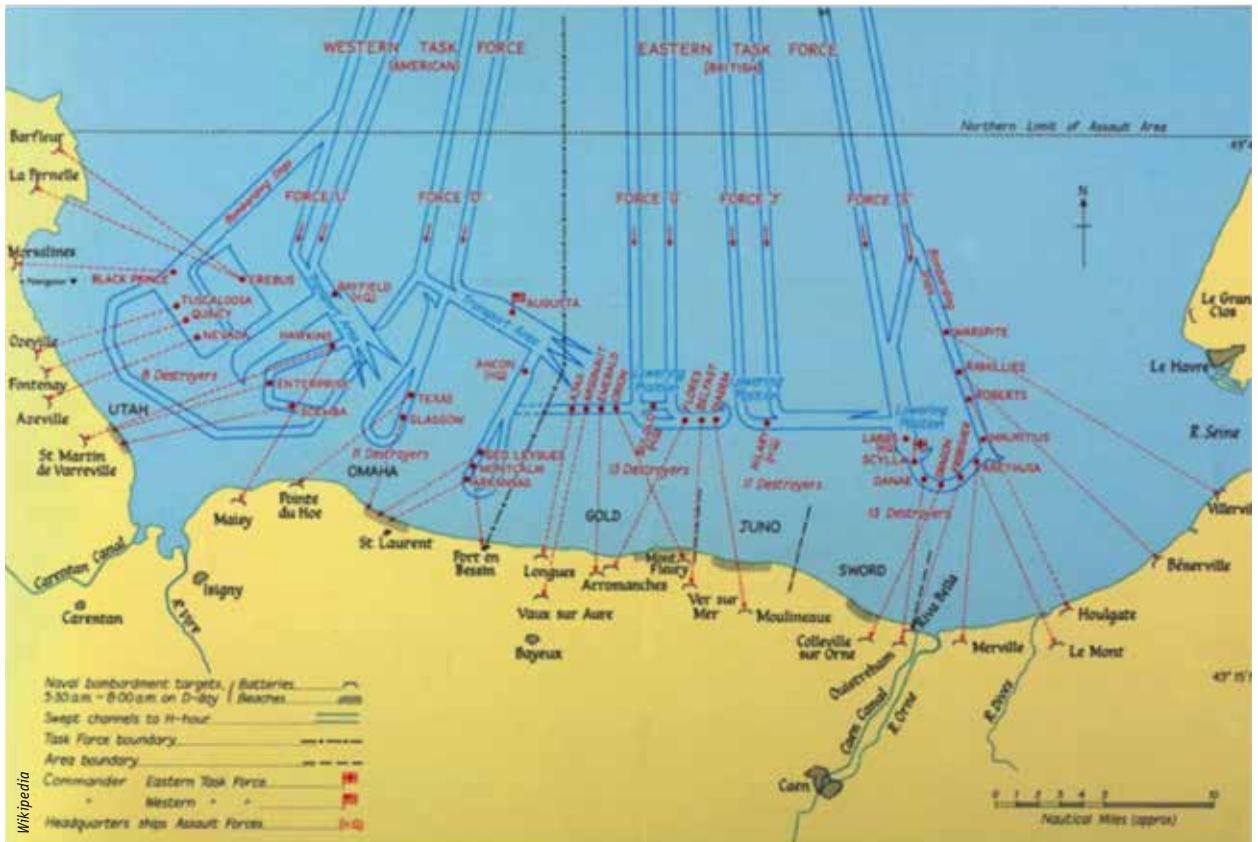
The goal of a stealthy, deceptive approach is to shape the adversary's decision-making processes through a false impression of the battlespace, and is

designed to lower an opponent's capabilities due to sub-optimal deployment of his finite resources.⁴ Simply put, deception is perception manipulation.

Military deception encompasses the use of both denial and deception, with denial as hiding the real and deception showing the fake. Within the military context, deception and its manifestations of propaganda and disinformation aim to deceive opponents as to the details of military operations: intentions, timings, locations, combat strength and style.⁵

The use of deception is well recorded in history. The concept of using the inferior to overcome the superior has its roots in ancient Chinese military history which emphasises stealth, deception and indirect approaches.⁶ In a recently declassified 1972 seminar by the United States (US) Joint Chief of Staff on intelligence warning function, a paper was presented on deception and surprise. The element of surprise was analysed in 168 battles in 17 wars from 1914 through 1968 and impressive statistics on the efficacy of deception were presented. Out of 50 battles in which intense surprise was achieved, 17 far exceeded the objectives of the initiators and only one ended in defeat. Conversely, out of the 50 battles fought without the advantage of initial surprise, 30 ended in defeat for the initiators and only one substantially exceeded the attacking commander's expectations.⁷ With 82% of all cases of strategic surprise and 57% of tactical surprises attributed to deception, the paper summarised that the greater the effort put into the deception plan, the greater the degree of surprise gained.⁸

In the following sections, three cases studies would be used to illustrate effective deception in the areas relevant to the SAF.



Naval Bombardments on D-Day, Operation Neptune.

STRATEGIC DECEPTION OF THE NORMANDY LANDINGS

A watershed moment in WWII was the Normandy Landings, codenamed Operation Neptune. The landing of two million men and thousands of ships and aircraft from around the world formed the largest joint and combined forces in history.⁹ It is one of the most successful in the history of warfare that is retold in countless documentaries and popular dramas such as HBO's *Band of Brothers*.

A key to the success of Operation Neptune was its elaborate deception plan, Operation Bodyguard. It had three main goals: to make the Pas de Calais appear to be the main invasion target, to mask the actual date and time of the assault and to keep German reinforcements in Pas de Calais for at least 14 days after landing. Operation Bodyguard was implemented as many sub-operations each focused on:

1. Military decoys and fake material/facilities pertaining to training and doctrine, for physical deception;
2. Controlled leaks of information through diplomatic channels;
3. Creating fake wireless traffic to simulate military units and operations;
4. Exploiting compromised agents to pass false information;
5. Media propaganda of phantom units such as the First United States Army Group (FUSAG) lent credibility by the supposed command of prominent US General George S. Patton.¹⁰

Operation Bodyguard was a success and it delayed the Fifteenth German Army in the Pas de Calais for seven weeks, exceeding the goal of 2 weeks. It has proven that with a well thought out and robustly executed deception plan, even a battle-hardened opponent can be deceived

by the crossing of two million soldiers across a large water obstacle like the English Channel.

OVERCOMING TECHNOLOGICAL INFERIORITY THROUGH DECEPTION

In the Kosovo Wars of 1999, the military of the Federal Republic of Yugoslavia (FRY) faced off with the North Atlantic Treaty Organisation (NATO) coalition for the control of Kosovo. Up against an adversary superior in all aspects of combat power, the FRY deception goal was to mitigate the superiority of the coalition's air force through the air campaign, Operation Allied Force, with efforts including staged media events employing a decoy military.¹¹

The military deception caused Allied aircraft to engage a variety of decoy targets, allowing FRY to conserve its limited tactical capabilities. Exploiting the Allied pilots' preference of using advanced thermal imaging for targeting, the FRY army fooled Coalition aircraft into attacking plywood and canvas targets tactically by using fires to create thermal images on bridges. These false thermal signatures emulated threat vehicles (tanks) exposed in the open on bridges, typically lucrative targets for Coalition aircrafts. Not only did it cost the Coalition to expand expensive smart munitions on cheap plywood, it lured NATO aircrafts into dangerous Surface-to-Air Missile (SAM) ambushes. The success of the FRY campaign was confirmed by its low losses from NATO's air campaign—only 20 tanks, 18 Armoured Personnel Carriers (APC) and 20 artillery pieces—a number significantly smaller than reported by NATO.¹²

Deception was used to influence the media reporting on the conflict. Examples of such media manipulation, to cast NATO in an evil light, included escorting reporters to non-military targets hit by

NATO aircraft but not to military ones and placing blood-stained dolls amongst civilian casualties whenever the international media photographed a site controlled by FRY.¹³

The goal of a stealthy, deceptive approach is to shape the adversary's decision-making processes through a false impression of the battlespace, and is designed to lower an opponent's capabilities due to sub-optimal deployment of his finite resources.

The FRY deception plan achieved its objectives: degrade the effectiveness of NATO air strikes; ensure the survival of Serbian forces; discredit NATO bombing campaigns; retain key foreign support by hiding or discrediting evidence of atrocities. This success, well documented in the open media, served as a source of embarrassment both for operational military planners and political leaders.¹⁴ It is an excellent example of how technological superiority can be eclipsed by a technologically-inferior adversary through the adroit deployment of deception.

DECEPTION BY BLURRING CIVIL MILITARY LINES

In August 2014, following the annexation of Crimea, Russian TV showed footage of water and baby food being loaded on to hastily repainted white trucks headed for Ukraine's war zone, as part of a humanitarian operation. Even though NATO has plenty of intelligence of Russian military movement of forces into Ukraine, Major General Davis, in charge of operations and intelligence at NATO's Headquarters, called the first convoy "a wonderful example of Maskirovka: because it created something of a media storm."¹⁵

TV crews breathlessly followed the convoy, trying to find out what was really inside the army trucks. To further fuel the media frenzy, Russian reporters staged interviews with the truck drivers to disprove speculation that a classic Trojan horse operation was ongoing to smuggle weapons to rebel militias in the Donbass region. However, The Trojan horse theory was reinforced by the distrust of the Russian media coupled with reports on social media showing that trucks supposedly loaded with humanitarian supplies were mostly empty. In response, the Ukraine military had to divert precious resources from their embattled army to screen the mostly empty trucks as they entered and left Ukraine. The true motive was to divert attention away from the movement of Russian forces and equipment at other checkpoints that were under the control of the Russians.

The brilliance of the masquerade was manifested in the media frenzy over the empty white army trucks, a self-sustaining smoke-screen for Russia perpetuated by the news-hungry Western media. Russian's constant blurring of military-civilian lines and its use of ambiguous forces throughout the Donbass conflict has enabled its operational success, even under the constant watch of the world and its military opponents.

INFORMATION DOMINANCE AND THE CO-EVOLUTION WITH DECEPTION

The Revolution in Military Affairs (RMA) concept envisioned information as a cornerstone of warfare, with modern militaries seeking information dominance by acquiring necessary information for friendly forces while denying it to the enemy.¹⁶ Dominating information is perceived as the key to dominating the entire battlespace. Vis-à-vis the advancement in sensor technologies, such as sub-meter, high resolution satellites, and the capabilities

to monitor the entire electromagnetic spectrum and electronic information channel, it is unfathomable that a modern military like the US, with its all-encompassing Command, Control, Communications, Intelligence, Surveillance and Reconnaissance (C4ISR) system, can be outfoxed by simple tactics such as empty trucks.

But the answer is simple, and can be found in biology; co-evolution, the concept of changes in the genetic composition of multiple species mutually affecting each other's evolution, explains the phenomenon.¹⁷ Deception, with its intrinsic association with information, has co-evolved with information operations. While the modern war-fighter and intelligence officer crave a comprehensive information collection system to enable pervasive battlespace awareness, the larger the coverage of the information systems, the greater are the venues for exploitation and deception effects.¹⁸ This leads us to an analysis of the media landscape, an ever-changing environment in which dominance is desirable, and deception thrives.

MEDIA 2.0: THE NEW TERRAIN

The evolving media landscape is a neutral terrain, open to all. Orit Perlov, a social media analyst for the Israeli-based Institute for National Security Studies, commented on the level playing field that is mainstream social media platforms: "Twitter is a very equalising platform, it's my voice and your voice, and the Prime Minister's voice ... Each one of us has 140 characters, no matter what. So it's a very democratic platform. It doesn't matter if you're black, white, left-wing, right-wing, your voice is the same."¹⁹

The American documentary maker Eugene Jarecki drew parallels between the histories of military and media supremacy. He cited George Orwell's

1945 essay, *'You and the Atom Bomb'*, in which Orwell argued that sophisticated weapons such as tanks, battleships and planes favour tyrants and oppressors, whereas accessible weapons such as rifles strengthen the weak.²⁰ The analogy was that cameras were big and expensive and only available to movie and television studios previously. As they have become cheaper and more available, ordinary people have gained control of the media narrative.²¹ Every potential player in a conflict, from individuals in the grassroots to Non-Government Organisations (NGOs) all the way up to governments and para-government organisations, now has a stake in the game in which they can potentially influence the public.²² The war-fighter plays by the same rules as everyone else.

This position is well-understood and effectively exploited. The media, in addition to the traditional military C4I system, forms an integral part of the modern information battlespace, what with its uses not just for influence, but also for Command and Control (C2) purposes. For example, Islamic State in Syria and Iraq (ISIS) generates 200,000 daily tweets from its supporters and members. It has 12 official accounts and 45,000 supporter accounts.²³ The terrorist group Al-Qaeda also uses encrypted e-mail exchanges and encrypted chat forums to communicate and disseminate its propaganda.²⁴ The level of technological sophistication rivals that of military secure communications, with a ubiquity and resilience that can surpass military C2 networks.

INFORMATION OPERATIONS IN MEDIA AND THE STRATEGIC CAMERAMAN

A modern military that understands the value of media in the information battlespace is the Israel Defense Forces (IDF). The IDF employs social media to great skill, with the IDF Spokesperson's

Unit established as the IDF's liaison to domestic and foreign media and the general public. When the unit first fired up its interactive media branch in December 2009, it started with only a few videos on YouTube. In 2014, it managed nearly 30 platforms speaking six languages—Hebrew, Arabic, English, Spanish, French, and Russian—with an estimated reach of 95 million people worldwide, a Twitter account with more than 230,000 followers and more than 380,000 likes on its Facebook page.²⁵

After taking out Hamas military leader Ahmed Jabari with a precision guided bomb, the IDF tweeted a chilling warning to Hamas: "We recommend that no Hamas operatives, whether low level or senior leaders, show their faces above ground in the days ahead," together with a tactical Unmanned Aerial Vehicle videos of the strike.²⁶ Not only does the IDF use media for propaganda, it uses it to debunk deception and false information created by its opponents. This is done by crowdsourcing to its followers, civilian and military alike, and the use of tools like Google image search and TinEye.²⁷ Despite the democratising power of social media, the media-savvy IDF's embrace of information operations demonstrates the value of social media for perception management.

Using video and photos to effectively present a story is also key to mastering the information domain. A case in point was the toppling of the statue of Saddam Hussein in Firdos Square, which marked the symbolic end of the Battle of Baghdad in the 2003 invasion of Iraq. The 'Strategic Corporal' of the moment, US Marine Corporal Edward Chin understood the strategic effects of toppling Saddam's statue.²⁸ However, it was the critical use of an Iraqi flag to cover the head of the statue that rallied the cheering Iraqi crowds into toppling



Minister for Defence, Dr Ng Eng Hen, trying out the controls of the Skyblade III unmanned aerial vehicle, one of the many surveillance equipment used by the C4I community.

the statue before the congregation of camera lens held by international journalists staying at the nearby Palestine Hotel.²⁹ The strategic cameraman understands not only the strategic act, but also the framing of it to leverage media to its purposes.

INFORMATION OPERATIONS OF THE 3RD GENERATION SAF

The 3rd Gen SAF prides itself on leading-edge capabilities that enable it to operate as a networked and integrated fighting force, effective across a full spectrum of operations. While the fighting system has been evolved to deliver precision and integrated strike capabilities, the SAF's holistic approach to transformation has also enabled the growth of its information operation capabilities.

The Defence Media Centre (DMC) is a multi-media, multi-platform agency dedicated to publishing defence-related content to inform, educate and engage Singaporean and international audiences about the Ministry of Defence (MINDEF) and the SAF. Besides its traditional flagship print products and corporate website, the DMC has begun tapping on the social media landscape to connect with its audience through YouTube, Facebook, Flickr and Twitter.³⁰ In addition, the SAF has established the Open Source Centre (OSC) under joint Imagery Support Group (ISG) to monitor global news and information related to military and security developments. It also tracks natural disasters in the region, such as Typhoon Hudhud over India and Typhoon Haiyan in the Philippines, using open source information on print, television and online news. The OSC sends its

reports to the highest SAF leadership twice daily on information from the open source channels.³¹

To enable information operations at the operational level, the SAF has developed specialised units such as the C4I battalions to support the combined arms brigade. The C4I battalion comprises information warfare specialists who provide comprehensive situational awareness and responsive information flows.³²

THE PANDORA'S BOX OF THE FUTURE

Revolutions in military affairs predict the civilianisation of conflict. The emergence of radical and quasi-state groups such as ISIS that possess heavy weaponry and state-sponsored use of 'little green men' by the Russian military in the annexation of Crimea, are evidence of the rapidly dissolving boundary between civilian and military. A preview into the predicaments

of the future would be the Russian Club-K containerised cruise missile system, commonly marketed as the 'Pandora's Box'. Packed in a standard shipping container, the weapon system can be fired from a container ship, a train cart or a container truck.³³ The Club-K blends into the urban environment and can be positioned covertly, ready to unleash a surprise attack at a moment's notice. Nothing on the exterior distinguishes the Club-K from a civilian container and this is an apt analogy for the future of conflict, in which there are no demarcations between civilians and military actors.

How should the SAF ready itself for a deceitful threat like the Club-K? There is no clear solution in the growing quagmire of civil-military relations in a conflict, but there will be growing emphasis on information operations. Information operations would be critical in tweezing out the weak signals of a deceptive threat among the growing cluttered environment. The recent



*Club K launchers at LIMA 2013, Langkawi.*³⁴

genesis of the SAF's C4I capabilities as a joint community highlights the awareness of the growing eminence of information operations.³⁵

To enable information operations at the operational level, the SAF has developed specialised units such as the C4I battalions to support the combined arms brigade.

TACTICAL INFORMATION OPERATIONS

This essay puts forth two suggestions for the decentralisation of information operations to the tactical level in anticipation of the future dynamic operating environment.

First, would be the use of combat media teams embedded with the frontline troops, similar to the combat production specialist vocation of the US Army.³⁶ As future operations are likely to be in the urban environment, there will be more interactions with civilian and non-combatants. They will be armed with a smartphone, eager to produce content to feed media hunger. The media teams will capture significant moments for documentation and operational learning purposes, but will also use them to debunk the aggressor propaganda of the SAF's operations or, to provide evidence in disputes with the civilians. The combat media teams must be combat capable, possess a good dose of creativity and media production flair, so as to capture the endearing moments while avoiding Public Relation (PR) disasters. The camera lens will shape the narrative of the operation and the strategic outcomes.

Next, would be the decentralisation of Intelligence Surveillance Reconnaissance (ISR) sensors, and intelligence reports, such as those generated by ISG's OSC. With the increase in urban operations, there will

be a decrease in situational awareness as it is limited by the human senses. To overcome these limitations would require sensors such as Signal Intelligence (SIGINT) and non-line of sight cameras such as tactical Unmanned Aerial Vehicles (UAV) to be made available to the front line troops. In addition, open sources and social media are rich sources of intelligence that should be constantly monitored. For example, the top-secret raid to kill Osama Bin Laden by the US Special Forces was exposed on Twitter by local residents as the raid unfolded.³⁸ The combat troops needed to be aware, as they moved from block to block, if their Operations Security (OPSEC) had been compromised on social media or whether there were signs of an Improvised Explosive Device (IED) waiting for a trigger signal.

The next generation SAF soldier needs to be information operations capable to operate in the dynamic and complex urban environment. Also, they need to have the acumen of an intelligence officer while being cognisant of the strategic goals of the SAF as they shape the battlespace with rifles and cameras.

CONCLUSION

This essay argues for the power of deception by highlighting key examples in modern military history. Deception thrives on information, and perception manipulation, and can be used to achieve operational surprise and to neutralise technological superiority.

The growing importance placed on information systems by modern militaries has brought about the co-evolution of deception techniques. The media has evolved into the new battlespace, where both deception and information dominance competes. A democratic field, media provides a voice to every actor, including the war fighter. It is thus important for modern militaries to be able to orchestrate information operations in the media: the strategic corporal gives raise to the strategic cameraman.

The 3rd Gen SAF is well aware of the needs of information operations as it undergoes its third generation transformation. There will be a push to further decentralise information operations down to the tactical levels. In the light of the blurring lines between civilian and military relations in conflict and the development of deceptive systems, the SAF must continue to transform to handle the perilous 'Pandora's Box' of the future. 🌐

BIBLIOGRAPHY

- 2LT Chan, P. Combating the Cognitive Trap of Mirror-Imaging: Pitfalls and Possibilities for the Intelligence Officer. (*POINTER*, 2014). 39-49.
- SAF's new team to pool intelligence operations. (*Asia One News*, 2012).
<http://news.asiaone.com/News/Latest+News/Singapore/Story/A1Story20120403-337338.html>
- Bin Laden raid was revealed on Twitter. (*BBC News*, 2011).
<http://www.bbc.com/news/technology-13257940>
- How Russia Outfoxes its enemies. (*BBC News*, 2015).
- Boey, D. (2010). MRAP unwrapped! <http://kementah.blogspot.sg/2010/07/mrap-unwrapped.html>
- Red Queen Hypothesis. C. M. Lively, Dept. of Biology, Indiana University.
http://www.indiana.edu/~curtweb/Research/Red_Queen%20hyp.html
- How Israel and Hamas weaponized social media. (*CNET*, 2014).
- COL Ong, Y. Understanding why inferior defeats the superior. (*POINTER*, 2008).
- CPT Guo, J. The Laments of Cassandra: Reflections on Warning Intelligence in the information Eden. (*POINTER*, 2006).
- Inauguration of the SAF C4I Community. (*Cyberpioneer*, 2012).
http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2012/apr/02apr12_nr.html#.VPR-KfmUfMJ
- Dr Ng visits SAF Imagery Support Group. (*Cyberpioneer*, 2014).
http://www.mindef.gov.sg:80/content/imindef/resourcelibrary/cyberpioneer/topics/articles/news/2014/oct/21oct14_news.html
- Flashpoint Global Partners. ICSR "Voices from the Blogs". (US CENTCOM, 2014).
- Gen Krulak, C. C. The Strategic Corporal: Leadership in the Three Block War. (*Marine Magezines*, 1999).
- Grabo, C. M., & Euan, D. G. (2009). Strategic Warning and Deception. Practice to deceive, 31-38.
<https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol16no4/pdf/v17i1a05p.pdf>
- Hosenball, M., & Whitesides, J. (2013). Reports on surveillance of Americans fuel debate over privacy, security. <http://www.reuters.com/article/2013/06/07/us-usa-wiretaps-verizon-idUSBRE95502920130607>
- MAJ Jon S Wendell. Strategic Deception Behind the Normandy Invasion. (United States Airforce: Command Staff College, 1997).
- MAJ Mark Johnson, & MAJ Jessica Meyeraan. *Military Deception: Hiding The Real – Showing The Fake*. (US Joint Forces Staff College, 2003)
- MAJ Seet, P. The Revolution in Military Affairs challenge to existing military paradigm and its impact on the Singapore Armed Forces. (*POINTER*, 2001).
- Introducing the C4I Battalions. (MINDEF, 2011).
http://www.mindef.gov.sg/imindef/mindef_websites/atozlistings/army/army_news/News_Archive/2011/Feb2011/c4ibn.html
- MINDEF. The Defence Media Centre
http://www.mindef.gov.sg/imindef/mindef_websites/atozlistings/dmc/index.html
- NATO. (2014). New Satellite Imagery Exposes Russian Combat Troops Inside Ukraine. <http://aco.nato.int/new-satellite-imagery-exposes-russian-combat-troops-inside-ukraine.aspx>
- Russian TV news. (2012). Twitter Warfare: How Israel and Hamas wage war online.

Szaszdi, L. F. The club K: A Deadly Pandora's Box of Cruise Missiles. (*The Daily Signal*, 2011) <http://dailysignal.com/2011/08/22/the-club-k-a-deadly-%E2%80%9Cpandora%E2%80%99s-box%E2%80%9D-of-cruise-missiles/>

The Isis propaganda war: a hi-tech media jihad. (*The Guardian*, 2014).

"I Shot 29 Bullets and 212 Images". (*Time*, 2012).<http://nation.time.com/2012/07/17/i-shot-29-bullets-and-212-images/>

U.S. Army. COMBAT DOCUMENTATION / PRODUCTION SPECIALIST (25V).

<http://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories/arts-and-media/combat-documentation-production-specialist.html>

United Nations Office on Drugs and Crime. The use of the Internet for terrorist purpose. (New York: United Nations, 2012).

Firdos Square statue destruction. *Wikipedia*. http://en.wikipedia.org/wiki/Firdos_Square_statue_destruction

Coevolution. *Wikipedia*. <http://en.wikipedia.org/wiki/Coevolution>

Global Surveillance. *Wikipedia*. http://en.wikipedia.org/wiki/Global_surveillance

Human Shield. *Wikipedia*. http://en.wikipedia.org/wiki/Human_shield

NATO bombing of Yugoslavia. *Wikipedia*. http://en.wikipedia.org/wiki/NATO_bombing_of_Yugoslavia

ENDNOTES

1. Sun Tzu, *Sun Tzu Quotes from the Art of War*, <http://www.artofwarquotes.com/>
2. How Russia Outfoxes its enemies, (*BBC News*, 2015).
3. Global Surveillance. *Wikipedia*. http://en.wikipedia.org/wiki/Global_surveillance
3. COL Ong, Y. Understanding why inferior defeats the superior. *POINTER*, v. 34, n. 1.
4. MAJ Mark Johnson, & MAJ Jessica Meyeraan. *Military Deception: Hiding the real - showing the fake*. US Joint Forces Staff College, (2003), 4.
5. Ibid.
6. Grabo, C. M., & Euan, D. G. *Strategic Warning and Deception. Practice to deceive*, (2009), 31.
7. Ibid., 32-33.
8. Major Jon S. Wendell. Strategic Deception Behind the Normandy Invasion. United States Airforce, Command Staff College. 1997.
9. Holt, Thaddeus. *The Deceivers: Allied Military Deception in the 2nd World War*. 2004.
10. NATO bombing of Yugoslavia. *Wikipedia*. http://en.wikipedia.org/wiki/NATO_bombing_of_Yugoslavia
11. MAJ Mark Johnson, & MAJ Jessica Meyeraan. *Military Deception: Hiding the real - showing the fake*. (US Joint Forces Staff College, 2003), 9.
12. Ibid., 10.
13. Ibid.
14. NATO. New Satellite Imagery Exposes Russian Combat Troops Inside Ukraine. <http://aco.nato.int/new-satellite-imagery-exposes-russian-combat-troops-inside-ukraine.aspx>, 2014.
15. How Russia Outfoxes its enemies. (*BBC News*, 2015).
16. Ibid.
17. Coevolution. *Wikipedia*.<http://en.wikipedia.org/wiki/Coevolution>.
18. CPT Guo, J. The Laments of Cassandra: Reflections on Warning Intelligence in the information Eden. (*POINTER*, 2006).
19. How Israel and Hamas weaponized social media. (*CNET*, 2014).
20. Orwell, George. You and the Atomic Bomb. http://orwell.ru/library/articles/ABomb/english/e_abomb.
21. The Guardian. The Isis propaganda war: a hi-tech media jihad. 2014.
22. How Israel and Hamas weaponized social media. (*CNET*, 2014).
23. Flashpoint Global Partners. ICSR "Voices from the Blogs". US CENTCOM. 2014.
24. United Nations Office on Drugs and Crime. The use of the Internet for terrorist purpose. (New York: United Nations, 2012).
25. How Israel and Hamas weaponized social media. (*CNET*, 2014).
26. Russian TV news. Twitter Warfare: How Israel and Hamas wage war online. 2012.

27. How Israel and Hamas weaponized social media. (*CNET*, 2014).
28. Gen Krulak, C. C. The Strategic Corporal: Leadership in the Three Block War. Marine Magazine. 1999.
29. Firdos Square statue destruction, *Wikipedia*.
http://en.wikipedia.org/wiki/Firdos_Square_statue_destruction, 2007.
30. MINDEF. The Defence Media Center.
http://www.mindef.gov.sg/imindef/mindef_websites/atozlistings/dmc/index.html.
31. Dr Ng visits SAF Imagery Support Group. (Cyberpioneer, 2014)
http://www.mindef.gov.sg:80/content/imindef/resourcelibrary/cyberpioneer/topics/articles/news/2014/oct/21oct14_news.html
32. MINDEF. Introducing the C4I Battalions.
http://www.mindef.gov.sg/imindef/mindef_websites/atozlistings/army/army_news/News_Archive/2011/Feb2011/c4ibn.html, 2011.
33. Szaszdi, L. F. The club K: A Deadly Pandora's Box of Cruise Missiles. (The Daily Signal, 2011).
<http://dailysignal.com/2011/08/22/the-club-k-a-deadly-%E2%80%9Cpandora%E2%80%99s-box%E2%80%9D-of-cruise-missiles/>.
34. Club K anti-ship missiles sold to South East Asia, Asitimes.
<http://asitimes.blogspot.sg/2013/04/club-k-anti-ship-missile-sold-to.html>, 2013.
35. Inauguration of the SAF C4I Community, Cyberpioneer.
http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2012/apr/02apr12_nr.html#.VPR-KfmUfMJ.
36. "I Shot 29 Bullets and 212 Images". (Time, 2012).
<http://nation.time.com/2012/07/17/i-shot-29-bullets-and-212-images/>, 2012.
U.S Army. Combat Documentation / Production Specialist (25V).
37. Bin Laden raid was revealed on Twitter. (*BBC News*, 2011).
<http://www.bbc.com/news/technology-13257940>



LTA(NS) Chin Hui Han is currently a Senior Member of Technical Staff at DSO National Laboratories. He graduated from Carnegie Mellon University with two Bachelors of Science degrees in Computer Science and Mathematical Science. LTA(NS) Chin is a Guards Officer by vocation.