Information Technology Advances: Friend or Foe?

by ME5 Su Juncun

Abstract:

Information Technology (IT) has advanced by leaps and bounds over the past few decades. In this essay, the author examines the implications of the advancement of IT on Singapore and the Singapore Armed Forces (SAF). He begins by tracing the rapid growth of IT, and along with it the evolution of cyber warfare, which has opened up a new battlefield in the realm of cyber space and shown the capability to facilitate psychological operations and perception management. On the other side of the coin, the author contends that IT has presented many new opportunities for the SAF to exploit, especially in the areas of learning and training, safety and administration and raising public awareness via social media platforms. By employing a combination of 'Quality' and 'Quantity' safety nets, the SAF may not only be able to counter the threats of cyber attacks, but also reap the many benefits of the advancements in IT to further enhance its effectiveness in defending the nation.

Keywords: Information Technology; Cyber Attacks; Social Media; Virtual Defence; Knowledge Management

INTRODUCTION

Information Technology and its History

IT is the use of systems to store, retrieve and send information.[1] It has come a long way: from clay tablets to preserve ancient Sumerian beer recipes 4,000 years ago, to the first telegram message tapped out by Samuel Morse from Washington to Baltimore in 1844.[2] Since then, IT has improved tremendously and taken new forms.[3]

The Invention and Global Proliferation of the Internet

By 1950, computers had been invented and in 1969, the first area network was operationalised, connecting several United States (US) universities.[4] It eventually evolved into the Internet — a system of networks that spans the globe today.[5] In 1990, there were around 300,000 Internet users. This number jumped to almost 3 billion in 2014.[6] The invention of computers and the Internet, and their derivatives, have since been regarded as the key IT advances in recent decades.

Jumping on the IT Bandwagon

Singapore jumped on the bandwagon in 1998. Then-Prime Minister, Mr Goh Chok Tong mentioned, "...that in order to stay ahead of competition, Singapore must aim to have a knowledge-based economy."[7] The government recognised that IT would play a crucial role and invested in extensive infrastructure development, e.g. the island-wide broadband.[8] This effort cumulated into the iN2015, a 10-year masterplan in May 2005, which was developed to grow the infocomm sector and technologies further.[9] By 2012, 84% of households had home broadband Internet access.[10]

Impact on National Defence: Susceptibility to Cyber Attacks

The world 'shrank' with IT advances. While this promoted economic growth in many countries, there were other complications. In the area of National Defence, it raises weighty questions about the possibility of Singapore and the Singapore Armed Forces (SAF) becoming more susceptible to cyber attacks.

> *"Technology... is a queer thing. It brings you great gifts with one hand, and it stabs you in the back with the other."*
>
> *-Carrie Snow*[11]

In this essay, the author aims to illustrate the potential adverse effects of cyber warfare on Singapore and the SAF; highlight the areas of opportunity for the SAF; and suggest possible defences against cyber attacks.

THE SNARES OF IT: CYBER WARFARE

Cyber Warfare is not new, but has evolved with IT advances

The importance of the control of information has existed since early history.[12] During the Napoleonic Wars, Emperor Napoleon I was defeated as his strategic sea communications were cut by the British Royal Navy.[13] This compromised the integrity of Napoleon's information environment.[14]

In this modern Information Age, cyber warfare has evolved and has been made potent by the Internet. The Internet is still the fastest communications system invented — it is easily accessible and grants users the protection of anonymity.[15] Therefore, where National Defence is concerned, Singapore and the SAF must not neglect the prowess of modern cyber warfare. The fight to control information will now comprise conventional warfare, cyber war and 'mental war.'[16] Any Singaporean or Singapore Armed Forces (SAF) serviceman may be drawn insidiously into this hybrid battlefield, right at their doorstep through IT.

Cyber war is Real and Implicates Decision-Making Processes

Cyber war, battle in the cyber space, controls information by wreaking havoc on IT systems. Between April 1990 and May 1991, five hackers from the Netherlands penetrated computer systems at American military sites and gained access to information about the US troop locations and weaponry details in the Gulf region.[17] While the hackers' primary objective was the profit from selling this classified information, they could have thwarted the US supplies and potentially altered the outcomes of the Gulf War by sending toothbrushes instead of bullets![18]

In 2007, the first documented case of cyber war intended to cause physical damage took place. A computer worm called Stuxnet was used to retard Iran's nuclear-weapons programmes at Natanz. Stuxnet turned valves on and off and meddled with the centrifuges, wasting uranium and damaging equipment.[19]

These examples illustrate some possibilities from a cyber war, but it could also affect the SAF's warfighting capability in another way. A potential adversary can slow down the SAF's decision-making process which would be instrumental in winning a war.[20] In this Information Age, information and its sources are aplenty and consequently, there are possible 'hackable' opportunities to upset the information that the SAF receives. Without the ability to confirm the veracity of the vast information received, the SAF would end up in a state of decision paralysis, needing to seek confirmation before deciding and acting.[21]

In 2013, online hacktivist group Anonymous launched a wave of cyber attacks on several Singapore-based websites, including The Straits Times.

Psyops and Perception Management

Cyber warfare can also take place in the 'mental space.' Psyops and perception management, which involve toying with the minds and behaviours of individuals, were already employed in the Gulf War where 70% of the Prisoners of War (POWs) reported that their decisions to surrender were influenced by the (psyops) leaflets.[22] A captured general shared that, "Second to the allied bombing campaign, psyop leaflets were the highest threat to the morale of the troops."[23] The Internet provides a convenient means of employing psyops and perception management through constructing a false reality in the cyber space. There exists a risk of an adversary uploading false information into one's databases in an attempt to influence undesirably.[24]

This can affect the SAF and the public as well.[25] As observed by Deputy Prime Minister Teo Chee Hean in 2014, "(We) are all also becoming increasingly dependent on cyber technologies for our daily activities, and the smooth and effective functioning of essential services. The cyber domain has thus become a lucrative target for those who aim to do harm."[26] In 2014 alone, we have seen major security breaches around the world. Globally, Sony Pictures Entertainment suffered from a major online attack while locally, karaoke entertainment operator K Box and Nanyang Polytechnic's databases were hacked.[27] In these cases, sensitive information was obtained and leaked. Therefore, it is not inconceivable that potential adversaries could hack similar computer systems, insert psyops 'e-leaflets' and influence the public and SAF servicemen unfavourably.

The Allure of Cyber Warfare – Affordable and Easily Propagated

Cyber warfare is cheaper and yet can be equally (if not more) potent. A cyber warfare team of 10 to 20 hackers using state-of-the-art computers could potentially accomplish the same objectives as a conventional military force to cause an enemy to

surrender.[28] The reality is sobering as modern IT has created new possibilities for offensive cyber warfare to take place in an instant, from anywhere in the world.[29]

The reality is sobering as modern IT has created new possibilities for offensive cyber warfare to take place in an instant, from anywhere in the world.

Against this backdrop, Singapore being rated second in the global Networked Readiness Index (NRI) would be especially vulnerable.[30] The advent of social media such as Facebook, Twitter and Youtube and its widespread usage in Singapore have exacerbated the problem.[31] Furthermore, the modern Information Age has seen the advent of digital devices. From computers to handphones and tablets, these devices allow faster Internet access, at greater convenience. They have created more opportunities for the world to invade and cause collateral damage unbeknown to us, in the form of malicious codes and viruses.[32]

THE SILVER LINING IN THE CLOUD OF IT ADVANCES

The advancement in IT is not just foe and no friend to the SAF. In fact, IT possesses immense potential and presents new opportunities for the SAF in the areas of learning and training, safety and administration and raising public awareness via the social media.

Learning and Training

IT advances present many avenues to enhance operational learning and training in the SAF. In 2009, Basic Military Training (BMT) recruits were issued laptops to access self-directed learning online tutorials before actual hands-on experience. These

Cyberpioneer

Tablet computers are employed in the SAF to enhance operation learning and training.

tutorials covered military fundamentals such as weapons handling and first aid procedures. In 2011, various SAF training institutes turned to the tablets, which made learning even more accessible.[33]

To enhance training realism, the Air Force Training Command has developed two simulators: the Virtual Reality Aircraft Recognition (VRAR) simulator which enables trainees to see aircraft approaches in three dimensions (3D); and the Virtual Hangar Trainer (VHT) which provides 3D virtual reality to train the maintenance crew on aircraft maintenance procedures and emergency response procedures.[34] The VHT also features recording functions and allow trainees to reflect, analyse and learn from their and others' mistakes.[35]

In the Republic of Singapore Navy (RSN), interactive online applications (apps) were built. For example, the 'Visual Signalling – Flashing' and 'Visual Signalling – Flag Hoisting' apps, developed in 2013, enabled naval communications trainees to learn key naval communications methods: transmitting Morse codes via light flashes and sending messages through flag hoisting. The apps allow self-learning, without the need of a dedicated instructor. With these apps, Headquarters Maritime Training and Doctrine Command was able to shorten the learning process and make lessons more effective.[36] Other examples include the US Marine Corps' pilots who use iPads loaded with digital maps. This has helped reduce their workload in the cockpit as they are now able to search for locations without the need to flip through bulky map packs.[37]

Safety and Administration

IT can enhance administrative and safety processes as well. Since 2013, certain administrative processes have been made easier with the launch of the 'MyNSAdmin' and the 'My eLeave and eClaims' apps. SAF Operationally-Ready National Servicemen (NSmen) can utilise the 'MyNSAdmin' app to notify the Ministry of Defence (MINDEF) of their overseas trips without needing to find a computer terminal. In addition, the app will automatically prompt the NSmen to do their overseas notification when they are at the airport or near any immigration checkpoint.[38] Via the 'My eLeave and eClaims' app, Full-Time National Servicemen (NSFs) also gained the flexibility of managing their annual leave plans and submitting transportation, medical and dental claims through their smartphones.[39]

Figure 1: 'My eLeave and eClaims' App[40]

To improve the management of safety, the 'Army Safety' app was launched in April 2014. Through this app, commanders and soldiers can quickly check on vital information such as weather conditions, location of nearby medical facilities and associated route information. "While (the app) does not replace any existing safety measures, it functions as a convenient

and complementary source of information," said CPT Muhd Noor Ehsan from the Army Safety Inspectorate (ASI). The app can also be used to report safety hazard reports to the ASI.[41]

Such public outreach not only generates awareness, but also promote positive images of the SAF in general. These have far-fetching effects such as enhancing the public's confidence and support of the SAF. It may even achieve some degree of deterrence effects.

Public Awareness through Social Media

As social media gains traction globally, the SAF has also leveraged on these platforms to create greater awareness and understanding of the SAF. One example is 'The Singapore Army' Facebook page. Managed by the Army Information Centre, this page shares stories, features, photos and videos about the Army. Interestingly, the page also features a summary of its history and key milestones since 1957.

When the Youtube series, 'Every Singaporean Son' first aired in 2010, it created much interest among the public, for this was the first time the SAF BMT in Pulau Tekong had been filmed and broadcasted. Said Mr. Donald Chew, Head of Defence Information

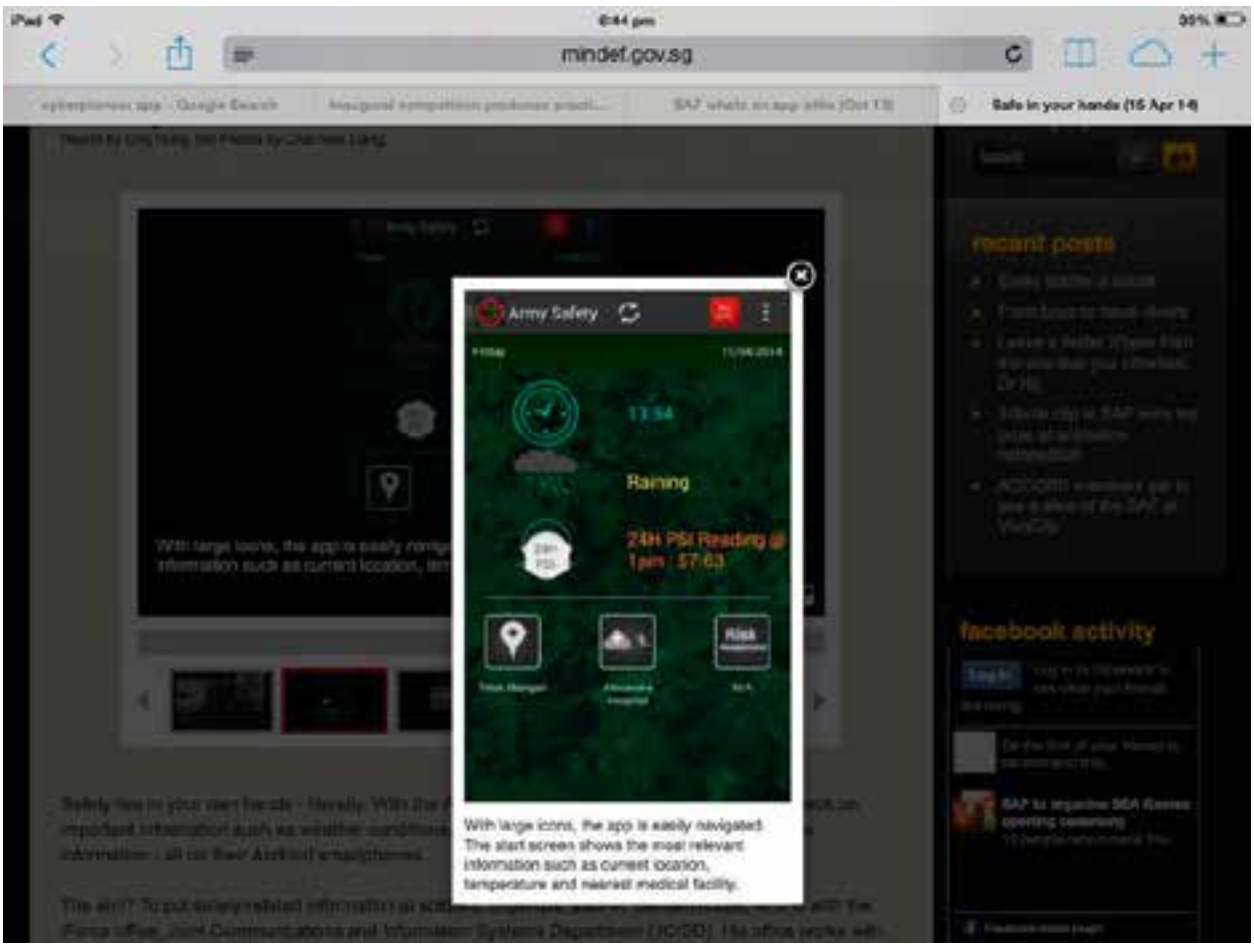

Figure 2: 'Army Safety' App[42]

Television, "We hope to get people to understand more about BMT."[43] Such public outreach not only generates awareness, but also promote positive images of the SAF in general. These have far-fetching effects such as enhancing the public's confidence and support of the SAF. It may even achieve some degree of deterrence effects.

SAFETY NETS

Virtual Defence

As Singapore becomes more networked and as the SAF continue to invest in more interoperable and networked infrastructure and systems, the relevance of virtual defence becomes more evident. This can also be seen in the US where the main threat to its Internet security is the sheer size of its Internet presence.[44] It will be increasingly difficult to keep out cyber warfare-capable adversaries. Nevertheless, resilient virtual defence can be and have been built to counter such threats. For instance, the US Department of Defense (DoD) employs strategies of both 'quantity' and 'quality' in building its Internet defences, by creating layers of defences with superior security software.[45] These form the backbone to the proposed virtual defence presented in the section below.

(I) Checks and Balances ('Quality' Strategy)

The IT workflows can be enhanced through appropriate policing and monitoring. Policing helps prevent information from being abused in a way that goes against the interests of security. This could be done by incorporating monitoring mechanisms that will provide the necessary checks and balances. Separately, there must also be safeguards against over-reliance on Artificial Intelligence, having machines talking to machines without a human supervising the conversation. Systems need to leave an aperture for control by humans to avoid the problems of passive neglect or runaway processing.[46]

(II) Be Ahead of the Game ('Quality' Strategy)

In building the virtual defence, the SAF must seek continuous improvements in order to stay ahead of the game, as the speed at which IT advances has outpaced current IT security solutions. Now, each IT security cycle begins with the use of the latest known effective software, and ends with the perfection of the newest escalation in attack mechanisms. The timeline for this cycle may soon be a matter of only hours.[47] As such, it is imperative that the SAF invests in Research and Development to stay ahead of this IT power curve. Another aspect is to share best practices and learn from other related agencies such as the Singapore Cyber Security Agency.[48]

(III) Be Extensively Armoured ('Quantity' Strategy)

Following the DoD's strategy of 'quantity', the SAF should also not 'put all its eggs in one basket'. In IT security terms, it translates to avoiding a single point of failure. By using a variety of layered virtual defences, information can be given the highest level of protection.

One of the major failure points is the inability to spot espionage or sabotage acts. A 'two-person control' would counter this vulnerability by setting up critical information workflows such that they must be executed by two (or more) persons. Examples include dual signatures or multiple authorisations. The rationale is that someone is less likely to abuse information if another person must be convinced to go along with the act.[49]

Backup systems are another way of preventing failures. Even if information or systems are sabotaged, there is an extra copy available. Any information should be backed up and protected against accident, natural disaster, or sabotage. Establishing reliable backup facilities is one of the main elements of a successful virtual defence system.[50]

(IV) Educated Servicemen ('Quantity' and 'Quality' Strategies)

To employ and execute virtual defence effectively, there must be proficient servicemen. In addition, humans are found to be the major vulnerabilities of IT security breaches. Education is therefore another important tenet to virtual defence. Security awareness and training programmes will serve to inform servicemen about the SAF's IT security policy, to sensitise them to risks and potential losses, and to train them in the use of security practices and technologies.[51]

In the current context of social media proliferation, the educational process should also emphasise the associated risks as well.[52] This, in the long run, will assist the SAF to build a quality IT security-savvy corps comprising of informed individuals who can provide the layered defences, such as the 'two-person' control, as discussed earlier.

Knowledge Management

On top of building a strong virtual defence, countering a cyber warfare battle also involves gaining an information advantage over the adversaries. One of the ways is to strengthen the decision-making process, through quicker, more thorough and better management of information. Effective Knowledge Management (KM) is one key enabler to this and may be associated with the use of a dynamic database, easily accessible applications and communications within an assured bandwidth. The goal is to blend the best intellects and IT available to turn information into knowledge faster than an adversary.[53]

Emergency Response Team

Last but not least, if the defences fail, the SAF must be prepared to react with an emergency response team. A reference would be the Singapore Computer Emergency Response Team (SingCERT), established in 1997 as a one-stop centre for security incident response in Singapore. It facilitates the detection, resolution and prevention of security related incidents on the Internet.[54] Another key service that SingCERT provides is collaborating with the industry, local and other national CERTs to resolve security incidents collectively. Having come a long way, the SingCERT, now known as the Cyber Security Agency since 2015, would be a worthy agency for the SAF to learn from.

CONCLUSION

"Good, bad or indifferent, if you are not investing in new technology, you are going to be left behind."

–Philip Green[55]

The advances in IT are unlikely to be reversed. Bearing in mind the inevitable global proliferation of IT, the world will 'shrink' further. The adverse effects of cyber warfare will become even more pertinent and perilous. In this setting, it is imperative that the SAF invests dedicated resources into IT security by building a combination of 'Quality' and 'Quantity' safety nets, managed and executed by informed servicemen. The SAF Cyber Defence Operations Hub, formed in 2013, is a good start as IT security experts are amalgamated under a single entity to counter digital warfare and beef up defences against online threats.[56]

In this setting, it is imperative that the SAF invests dedicated resources into IT security by building a combination of 'Quality' and 'Quantity' safety nets, managed and executed by informed servicemen.

The logical way forward would be to take advantage of the many opportunities afforded by IT advances. The SAF will be able to enhance aspects such as learning and training, safety and administration and also harness other intangible positive outcomes from raising public awareness through the use of social media.

BIBLIOGRAPHY

"Annual Survey on Infocomm Usage in Households and by individuals for 2012," (*Infocomm Development Authority of Singapore*, 2015), http://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Facts%20and%20Figures/SurveyReport/2012/2012HHmgt.pdf.

Berkowitz, Bruce D. *The New Face of War: How War Will Be Fought in the 21st Century*. New York: Free Press, 2003.

Bilbao-Osorio, Beñat, Dutta, Soumitra and Lanvin, Bruno, Editors, "Rewards and Risks of Big Data", *The Global Information Technology Report 2014*, 2014.

Campen, Alan D. *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Fairfax, Va.: AFCEA International Press, 1996.

Chow, Jermyn, "SAF Sets up New 'Cyber Army' to Fight Digital Threats," (*The Straits Times*, 2013), http://www.straitstimes.com/breaking-news/singapore/story/saf-sets-new-cyber-army-fight-digital-threats-20130630.

Denning, Dorothy Elizabeth Robling, *Information Warfare and Security*, New York: ACM Press, 1999.

Dunnigan, James F. *The Next War Zone: Confronting the Global Threat of Cyberterrorism*. New York: Citadel Press, 2002.

"Every Singaporean Son," (*MINDEF*, 2010), http://www.mindef.gov.sg/imindef/resourcelibrary/videos/docus/evrySporeanSon.html#.VOsZC_lhuSp.

Fu Wei'en Eugene and Nah Jinping, "Understanding the Millennial Generation: Developing a More Effective Workforce for the Future SAF", *POINTER*, v._39, n._ 1, 2013.

Hall, Wayne M. *Stray Voltage: War in the Information Age. Annapolis*, Md.: Naval Institute Press, 2003.

"How Cyber War-fare Really Started – and Where it will lead," (*The Economist*, 2014), http://www.economist.com/news/books-and-arts/21635967-how-cyber-warfare-really-startedand-where-it-will-lead-turning-worm.

"iN2015 Masterplan," (*Infocomm Development Authority of Singapore*, 2014), http://www.ida.gov.sg/Infocomm-Landscape/iN2015-Masterplan.

Infocomm Development Authority of Singapore, "Infocomm Usage – Households and Individuals," 2014, Selected Primary Internet Activities by Age Group (2012) – Communication Activities, http://www.ida.gov.sg/Infocomm-Landscape/Facts-and-Figures/Infocomm-Usage-Households-and-Individuals#7.

"Infocomm Security," (*Infocomm Development Authority of Singapore*, 2014), http://www.ida.gov.sg/Infocomm-Landscape/Infocomm-Security.

Kwang, Kevin, "5 Security Threats to Watch Out for in 2015", (*Channel News Asia*, 2014), http://www.channelnewsasia.com/news/technology/5-security-threats-to/1534772.html.

Kwang, Kevin, "Cyber Warfare needs a 'Geneva Convention': Israel's Space Agency Chairman," (*Channel News Asia*, 2014), http://www.channelnewsasia.com/news/singapore/cyber-warfare-needsa/1421010.html.

Lee Hsiang Wei, "Managing the Risks of Social Media in the SAF", *POINTER*, v._39, n._2, 2013.

Leong Wai Kit, "Seven Cyber Security Projects to get Funding Boost from NRF," (*Channel News Asia*, 2014), http://www.channelnewsasia.com/news/singapore/seven-cybersecurity/1415680.html.

Lieutenant General John L. Woodward, Jr, "Statement of: Lieutenant General John L. Woodward, Jr, USAF Deputy Chief of Staff, Communications and Information United States Air Force on Information Assurance," (*The Information Warfare Site*, 2001), http://www.iwar.org.uk/cip/resources/ia-hearing-2001-05/01-05-17woodward.htm.

Lur, Xavier, "SAF to arm new recruits with iPADS," (*Yahoo News*, 2011), https://sg.news.yahoo.com/blogs/fit-to-post-technology/saf-arm-recruits-ipads-093835831.html.

"Nanyang Polytechnic Alumni Database Breached, Bank Details Stolen", (*Channel News Asia*, 2015), http://www.channelnewsasia.com/news/singapore/nanyang-polytechnic/1648374.html

Ng Wei-Jin, "Overcoming Digital Turbulences for the 3rd Generation RSAF," (*POINTER*, 2010), http://www.mindef.gov.sg/content/imindef/publications/pointer/journals/2009/v35n1/feature5.html.

Ong Hong Tat, "Safe in Your Hands," (*MINDEF*, 2014), http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/news/2014/apr/15apr14_news2.html#.VOrhY0cT4h.

Ong Hong Tat, "Transforming Learning," (*MINDEF*, 2012), http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/features/2012/aug12_fs2.html#.VOsVb40cT4g.

Quinn, Matt and Taylor, Chris, "Managing Big Risks and Rewards of Big Data," *The Global Information Technology Report 2014*, 2014.

"Social Analytics (SA) for Business Enterprises Call-for-Collaboration (CFC)," (*Infocomm Development Authority of Singapore*, 2013), http://www.ida.gov.sg/Collaboration-and-Initiatives/Collaboration-Opportunities/Store/Social-Analytics-SA-for-Business-Enterprises-Call-for-Collaboration-CFC.

"Statement by 2nd Minister at COS Debate 2007," (*Infocomm Development Authority of Singapore, 2007*), https://www.ida.gov.sg/About-Us/Newsroom/Speeches/2007/20060822111238.aspx.

Tan Guan Wei, "SAF Whets an App-etite," (*MINDEF*, 2013), http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/features/2013/oct13_cs.html#.VOr6D_lhuSr.

ENDNOTES

1. "Definition of Information Technology," (*Oxford University Press*, 2014), http://www.oxforddictionaries.com/definition/english/information-technology.
2. Bruce D. Berkowitz, *The New Face of War: How War Will Be Fought in the 21st Century*, New York: Free Press, 2003, 1-2.
3. Ibid.
4. The Advanced Research Project Agency Network (ARPANET). Dorothy Elizabeth Robling Denning, *Internet Besieged: Countering Cyberspace Scofflaws, New York: ACM Press*, 1998, 15-27.
5. Dorothy Elizabeth Robling Denning, I*nternet Besieged: Countering Cyberspace Scofflaws*, New York: ACM Press, 1998, 15-27.
6. Victor Luckerson, "Internet Users Surge to Almost 3 Billion Worldwide," (*TIME*, 2014), http://time.com/3604911/3-billion-internet-users/.
7. Goh Chok Tong, "S'pore Gears up for New Growth Wave," Address at the Opening Dinner at the World Economic Forum's annual East Asia summit on 13 October 1998, The Straits Times, 1998.
8. Ibid.
9. "iN2015 Masterplan," (*Infocomm Development Authority of Singapore*, 2014), http://www.ida.gov.sg/Infocomm-Landscape/iN2015-Masterplan.
10. "Annual Survey on Infocomm Usage in Households and by individuals for 2012," (*Infocomm Development Authority of Singapore*, 2015), http://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Facts%20and%20Figures/SurveyReport/2012/2012HHmgt.pdf.
11. Carrie Snow, "Carrie Snow Quotes," *Brainyquote*, http://www.brainyquote.com/quotes/quotes/c/carriesnow108049.html.
12. James F. Dunnigan, *The Next War Zone: Confronting the Global Threat of Cyberterrorism*, New York: Citadel Press, 2002. 104-110.
13. John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" *Comparative Strategy*, v._12, 1993, 141-165.
14. Loyal Rue, *By the Grace of Guille: the Role of Deception in National History and Human Affair*, Oxford University Press, New York, 1994, 120-122.
15. James F. Dunnigan, *The Next War Zone: Confronting the Global Threat of Cyberterrorism*, New York: Citadel Press, 2002. 104-110.
16. Michael L. Brown, "The Revolution in Military Affairs: The Information Dimension," in *Cyberwar: Security, Strategy, and Conflict in the Information Age*, Campen, Alan D., Fairfax, Va.: AFCEA International Press, 1996, 43.
17. Dorothy Elizabeth Robling Denning, *Information Warfare and Security*, New York: ACM Press, 1999, 3-4.

18. Gina Smith, "Hackers Could Switch Toothbrushes for Bullets," (*ABCNews.com*, 1997).

19 . "How Cyber War-fare Really Started – and Where it will lead," (*The Economist*, 2014), http://www.economist.com/news/books-and-arts/21635967-how-cyber-warfare-really-startedand-where-it-will-lead-turning-worm.

20. Typically takes the form of an OODA (Observe, Orient, Decide and Act) loop.

21. Wayne M. Hall, *Stray Voltage: War in the Information Age, Annapolis*, Md.: Naval Institute Press, 2003, 25.

22. John Petersen, "Information Warfare: The Future," in Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, eds., *Cyberware: Security, Strategy and Conflict in the Information Age, AFECEA International Press, Fairax*, VA, 1996, 219-226.

Stephen T. Hosmer, *Psychological Effects of US Air Operations in Four Wars 1941 – 1991*, Rand, Santa Monica, CA, 1996, 143-148.

23. Chad R. Lamb, "Military Psychological Operations," term paper for COSC 511, May 4, 1997, citing "US Army Special Forces: The Green Berets – US Special Operations Command: Psychological Operations," http://users.aol.com/armysof1/PSYOPS.html.

24. Michael L. Brown, "The Revolution in Military Affairs: The Information Dimension," in *Cyberwar: Security, Strategy, and Conflict in the Information Age, Campen*, Alan D., Fairfax, Va.: AFCEA International Press, 1996, 46.

25. John Rendon, "Mass Communication and Its Impact," in National Security in the Information Age, James P. McCarthy ed., Conference Report, US Air Force Academy, February 28-March 1, 1996.

26. Leong Wai Kit, "Seven Cyber Security Projects to get Funding Boost from NRF," (*Channel News Asia*, 2014), http://www.channelnewsasia.com/news/singapore/seven-cybersecurity/1415680.html.

27. Kevin Kwang, "5 Security Threats to Watch Out for in 2015," (*Channel News Asia*, 2014), http://www.channelnewsasia.com/news/technology/5-security-threats-to/1534772.html.

"Nanyang Polytechnic Alumni Database Breached, Bank Details Stolen," (*Channel News Asia*, 2015), http://www.channelnewsasia.com/news/singapore/nanyang-polytechnic/1648374.html.

28. Dorothy Elizabeth Robling Denning, *Information Warfare and Security*, New York: ACM Press, 1999, 17.

29. Ibid.

30. Beñat Bilbao-Osorio, Soumitra Dutta and Bruno Lanvin, "Rewards and Risks of Big Data," *The Global Information Technology Report 2014*, 9-15.

31. "Social Analytics (SA) for Business Enterprises Call-for-Collaboration (CFC)," (*Infocomm Development Authority of Singapore*, 2013), http://www.ida.gov.sg/Collaboration-and-Initiatives/Collaboration-Opportunities/Store/Social-Analytics-SA-for-Business-Enterprises-Call-for-Collaboration-CFC.

32 . Symantec's Vice-President of Product Management for Mobility Michael Lin told Channel NewsAsia that mobile malware has risen by about 300 times in the past year. He added that the company's mobile application (app) insight tool, which inspects 15 million apps in 40 per cent of Android app stores, found that about 900,000 apps had malicious code in them. Kevin Kwang, "5 Security Threats to Watch Out for in 2015," (*Channel News Asia*, 2014), http://www.channelnewsasia.com/news/technology/5-security-threats-to/1534772.html.

Ng Wei-Jin, "Overcoming Digital Turbulences for the 3rd Generation RSAF," (*POINTER*, 2010), http://www.mindef.gov.sg/content/imindef/publications/pointer/journals/2009/v35n1/feature5.html.

33. Xavier Lur, "SAF to arm new recruits with iPADS," (*Yahoo News*, 2011), https://sg.news.yahoo.com/blogs/fit-to-post-technology/saf-arm-recruits-ipads-093835831.html.

34. Ng Woon Teck Ryan, "A Maintenance Simulator for Air Force Engineers: The RSAF Experience," *IAL Adult Learning Symposium 2014*, 2014.

35. Ibid.

36. Tan Guan Wei, "SAF Whets an App-etite," (*MINDEF*, 2013), http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/features/2013/oct13_cs.html#.VOr6D_lhuSr.

37. Xavier Lur, "SAF to arm new recruits with iPADS," (*Yahoo News*, 2011), https://sg.news.yahoo.com/blogs/fit-to-post-technology/saf-arm-recruits-ipads-093835831.html.

38. Tan Guan Wei, "SAF Whets an App-etite," (*MINDEF*, 2013), http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/features/2013/oct13_cs.html#.VOr6D_lhuSr.

39. Ibid.

40. Ibid.

41. Ong Hong Tat, "Safe in Your Hands," (*MINDEF*, 2014), http://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/news/2014/apr/15apr14_news2.html#.VOr-hY0cT4h.

42. Ibid.

43. "Every Singaporean Son," (*MINDEF*, 2010), http://www.mindef.gov.sg/imindef/resourcelibrary/videos/docus/evrySporeanSon.html#.VOsZC_lhuSp.

44. James F. Dunnigan, *The Next War Zone: Confronting the Global Threat of Cyberterrorism*, New York: Citadel Press, 2002. 253.

45. Ibid.

46. Matt Quinn and Chris Taylor, "Managing Big Risks and Rewards of Big Data," *The Global Information Technology Report 2014*, 64.

47. Alan D. Campen, *Cyberwar: Security, Strategy, and Conflict in the Information Age, Fairfax*, Va.: AFCEA International Press, 1996, 280.

48. Kevin Kwang, "Cyber Security Agency will spur 'pro-active' security-first mindset among firms: Yaacob", (*Channel News Asia*, 2015), http://www.channelnewsasia.com/news/business/cyber-security-agency/1678994.html.

49. Dorothy Elizabeth Robling Denning, *Information Warfare and Security*, New York: ACM Press, 1999, 384.

50. Ibid.

51. Ibid., 382.

52. Lee Hsiang Wei, "Managing the Risks of Social Media in the SAF", *POINTER*, v._39, n._ 2, 2013, 19.

53. Wayne M. Hall, *Stray Voltage: War in the Information Age, Annapolis*, Md.: Naval Institute Press, 2003, 132.

54. "Infocomm Security," (*Infocomm Development Authority of Singapore*, 2014), http://www.ida.gov.sg/Infocomm-Landscape/Infocomm-Security.

55. Philip Green, "Philip Green Quotes," *Brainyquote*, http://www.brainyquote.com/quotes/quotes/p/philipgree622050.html.

56. Jermyn Chow, "SAF Sets up New 'Cyber Army' to Fight Digital Threats," (*The Straits Times*, 2013), http://www.straitstimes.com/breaking-news/singapore/story/saf-sets-new-cyber-army-fight-digital-threats-20130630.

ME5 Su Juncun is an Air Force Engineer by vocation and is currently serving as an Officer Commanding in 806 Squadron, Air Power Generation Command. He was awarded the SAF Academic Scholarship and graduated with a degree in Mechanical Engineering (Honours, 2nd Class Upper) from the National University of Singapore. ME5 Su's previous appointments included two postings in 6th Air Engineering and Logistics Group, and a staff appointment in Air Engineering and Logistics Department.