BOOK REVIEW – THERE WILL BE CYBER WAR

Jonathan Lim
Australian National University

Details:

Title:	There Will Be Cyberwar: How The Move To Network-Centric War Fighting Has Set The Stage For Cyberwar
Author:	Richard Stiennon
Place of Publication:	1221 Bowers, #1274, Birmingham, MI 48009
Publisher:	IT-Harvest Press
Date of publication:	2015
Number of pages:	174
Price:	$9.79 (paperback)
ISBN-13:	978-0-9854607-8-5

Introduction

Richard Stiennon's *There Will Be Cyberwar: How the Move to Network-Centric War Fighting Has Set the Stage for Cyberwar* provides an intricate perspective into the emergent threats faced by governments in the cyber realm, and emphasizes how the constant lethargy and reactive approach of governments toward cybersecurity heralds the inevitability of a "cyber Pearl Harbor".

Stiennon is an industry analyst, adviser, and security executive with 20 years' experience in subjects such as cybersecurity, governance, risk and compliance, and analytics within the technology research industry. He was previously the Director of Cyber Security for Kaiser Permanente, where he ran one of the industry's first security data science teams focused on advanced threat detection. He has also held leadership roles in several venture capital backed security organization and insurance firms, was a founder of RustNet, and worked as an ethical hacker for PricewaterhouseCoopers.[1] These experiences have provided him with a broad perspective on how the IT industry

1 RSA Conference, 'Richard Stiennon', *RSA Conference*, 27 December 2015), https://www.rsaconference.com/speakers/richard-stiennon.

operates, and how bureaucracies have responded to emergent cyber threats. Stiennon has been writing and speaking about cyber security since 1995, and is the current General Manager of Cyber Security & Privacy for GE Healthcare, and Chief Research Analyst at IT-Harvest. It has been Steinnon's intention to contribute his perspectives to advancing cybersecurity throughout both the government and business sectors, through this book.

Steinnon reveals how the rapid and reckless adoption of technology by the United States military has been a double-edged sword, one which has multiplied the ability of the US to project power instantaneously across the globe to maintain its military industrial complex and superpower status, and which has simultaneously opened vulnerabilities within its military infrastructure, and threatens to overturn the balance of power on the battlefield. This proliferation of technology within the military to affect a competitive advantage is termed Network Centric Warfare (NCW). While the US remains the world's foremost cyber super power, its national critical infrastructure is prone to debilitating attacks within future conflicts unless immediate proactive measures are taken to affect the forward consideration of attack methodologies.

The book spans 174 pages and 18 chapters in total, including its bibliography. While there is a notable absence of any visual materials, there is an established scholarly apparatus through its table of contents, frequent use of referencing indicators, and inclusion of citations at the end. This provides sufficient background information for readers to conduct further research.

Context

This book represents a concise introductory text to the world of network centric warfighting and an updated view of cyber affairs within the military and IT industry. The book builds upon his previous works including *Surviving Cyberwar* (Rowman&Littlefield, 2010) and *UP and to the RIGHT: Strategy and Tactics of Analyst Influence* (IT-Harvest Press, 2012), seeking to amend the contentions on cyber espionage and cyber war within the former with geopolitical developments since 2010, and incorporating the technical expertise and industry knowledge demonstrated within the latter. *There Will by Cyberwar* provides a strong basis for further reading within Fred Kaplan's *The Secret History of Cyberwar* (Simon&Schuster, 2017), which provides a more comprehensive analysis of the wider historical basis of cyberwarfare and reveals how the US government remains unprepared against a resourceful cyberattack. Steinnon's book provides a competent foundation for further research into various fields of international affairs, including international security, outer space, and international humanitarian law.

There Will be Cyberwar represents Steinnon's most recent published work and it became a Washington Post Best Seller in April 2016. It reveals vulnerabilities within the military Internet of Things (IoT).. and illustrates the evolution of cyber weapons, emphasizing the fatal reactive pattern of governments and businesses towards cyberattacks, and highlights how organizations must maintain constant vigilance of developments in cyberspace.

Analysis

In its opening the book presents a hypothetical US military operation in the Taiwan Straits through the eyes of a post-event Congressional committee on the incident. This was premised on the desire to deter China's assertive moves and reaffirm US commitment to its allies in East Asia by moving its carrier fleets into the Taiwan Straits. The event was preceded by a series of calculated espionage operations, with communications encryption keys being stolen, GPS signals being spoofed, active bugs preventing the deployment of weapons systems, and communications channels exploited to facilitate deception. This was followed by a catastrophic cascade of events resulting in the decimation of US military forces in East Asia, the invasion and loss of Taiwan, and international concern over US capacity to maintain its security commitments.

This dramatic geopolitical scenario serves as a detailed demonstration into how the US military's persistent vulnerability to crippling cyberattacks could degrade or destroy its offensive and defensive capabilities within conflict zones, resulting in a lost battle, a change in military standing, and a shift in geopolitical balance. In its closing remarks, the comments by the fictional congressional committee provide a learned insight into what is required to avoid such an incident in the future; including a secure supply chain, continuous software and vulnerability reviews, and strong authentication measures. While prima facie the scenario appears implausible, if not highly unlikely, the underlying chain of events contributing to this eventuality have been validated by China's state-sponsored espionage operation "Titan Rain"[2] and its theft of weapons blueprints from the US Defense Industrial Base in 2013.[3]

Steinnon proposes his definition of cyberwar as "the use of computer and network attacks to further the goals of a war-fighting apparatus" and encompassing both computer network attacks (CNA) and exploitation (CNE). He deliberately chose this definition to constrain cyberwar to the military use of computers and network attacks while leaving open the possibility of non-

2 Council on Foreign Relations, 'Titan Rain' *Council on Foreign Relation*s, 2018, https://www.cfr.org/interactive/cyber-operations/titan-rain.

3 Ellen Nakashima, "US weapon plans compromised by China: report" *The Sydney Morning Herald,* 28 May 2013, https://www.smh.com.au/technology/us-weapon-plans-compromised-by-china-report-20130528-2n8gn.html.

state actors such as terrorists and violent activists, thus leading readers on a structured explanation of how the move toward NCW has set the basis for cyberwar. Indeed, where a definition of "Cyberwar" in law and legal convention is absent, traditional law of war concepts have been applied to cyber operations.[4] Steinnon's analysis would have benefited from reference to the legal and geopolitical implications of a set definition of "Cyberwar", particularly concerning the relevant customary international principles contained within the Tallinn Manual 2.0, with acute reference to the emergent dichotomy between "cyberwarfare" and "cyber operations," as many cyberattacks commonly reside beneath the threshold at which international law would consider them a formal act of war.[5]

To reinforce his thesis on vulnerabilities within military technology, Steinnon argues that the military is prone to cyber vulnerabilities in its often-reckless rush to network its systems and maintain its technological advantage. This has in turn resulted in the lack of safety precautions in the pillars of NCW; weapons systems, battle management systems, command and control networks, and Intelligence, Surveillance and Reconnaissance (ISR) communications. Steinnon crafts a coherent narrative outlining how this circumstance has transformed US military operations. He recounts the efforts of Admiral Archie Clemins to bring the US Navy into the information age, outfitting the US Navy's 7th Fleet with IT infrastructure in the form of Windows 95 PCs. The employment of NCW thus enabled the US to respond instantaneously to developments on the ground during the Third Taiwan Strait Crisis in March 1996, reassuring Taiwan and underlining US commitment to its allies against China. However, subsequent vulnerabilities within NCW were exposed followed by the 2001 Hainan Island Incident, where China's capture of a Navy EP-3E plane over the South China Sea provided them with the operating system and techniques employed by the NSA and resulted in the compromise of the US intelligence communications links in 2008.[6]

Steinnon illustrates how the US mismanagement of cyber and electronic security measures has been an persistent issue which lead to the loss of US military drones to Iran in 2011 and 2013,[7] ships using spoofed automatic

4 Lisa Brownlee, "Why Cyberwar is so hard to define" *Forbes*, 16 July 2015, https://www.forbes.com/sites/lisabrownlee/2015/07/16/why-cyberwar-is-so-hard-to-define/#6edab9d431f1.

5 Klav Leetaru, "What Tallinn Manual 2.0 Teaches Us About The New Cyber Order" *Forbes* (9 February 2017) https://www.forbes.com/sites/kalevleetaru/2017/02/09/what-tallinn-manual-2-0-teaches-us-about-the-new-cyber-order/#32d34fc4928b.

6 Kim Zetter, "Burn After Reading," *The Intercept*, 10 April 2017, https://theintercept.com/2017/04/10/snowden-documents-reveal-scope-of-secrets-exposed-to-china-in-2001-spy-plane-incident/.

7 "Iran airs images allegedly extracted from U.S. drone," *USA Today*, 7 February 2013, https://www.usatoday.com/story/news/world/2013/02/07/iran-cia-spy-drone-footage/1898011.

identification systems,[8] insurgents intercepting live video feeds from US Predator drones,[9] and the infiltration of the Secret Internet Protocol Routing Network (SIPRNet is a global communications network employed by defense contractors) by a number of viruses among others.[10] Steinnon's criticism of the US military's lax approach to cybersecurity remains relevant two years onward, with the Navy suffering a series of suspicious and fatal ship collisions– the USS John S. McCain colliding with a civilian ship in the Straits of Malacca and the USS Fitzgerald colliding with civilian ships off the coast of Japan.[11]

Steinnon's primary thesis is predicated on a cylcle repeated throughout history: technology is developed, then an attack is developed, followed by defense being developed. The results is a persistent shortcoming that security measures are rarely built into new technologies, thus jeopardizing critical national infrastructure systems such as industrial control systems, medical devices, transportation, and the pillars of NCW. Two years after publication, Steinnon's thematic predictions were validated by the May 2017 WannaCry ransomware attack, a worldwide cyberattack which spread through an exploit present in older Windows Systems and constituted one of the largest cyberattacks in history—with 200,000 computers across 150 countries affected and total damages amounting to billions of dollars.[12]

Steinnon suggests a few strategies which may be assumed by the US military to address its current cybersecurity weaknesses, including bolstering cyber supply-chain security, adopting more pervasive use of encryption with strong key management, operational and system hardening, and continuously monitoring all network traffic. This is accompanied by the doctrine of the Cyber Kill Chain developed by Lockheed Martin, a form of cyber triage which breaks down each stage of a malware attack into seven defined levels where victims can identify and stop a cyberattack.[13] Steinnon also suggests the wide

8 Tim Simonite, "Ship Tracking Hack Makes Tankers Vanish from View," *MIT Technology Review,* 18 October 2013, https://www.technologyreview.com/s/520421/ship-tracking-hack-makes-tankers-vanish-from-view/

9 Siobhan Gorman and Yochi J. Dreazen, August Cole, "Insurgents Hack US Drones" *Wall Street Journal*, 17 December 2009, https://www.wsj.com/articles/SB126102247889095011.

10 Noah Shachtman, "Under worm assault, military bans disks, USB drives," *Wired*, 19 November 2008, https://www.wired.com/2008/11/army-bans-usb-d/.

11 Sean Gallagher, "USS McCain collision ultimately caused by UI confusion," *ArsTechnica*, 3 November 2017, https://arstechnica.com/information-technology/2017/11/uss-mccain-collision-ultimately-caused-by-ui-confusion/; Luis Martinez, "USS Fitzgerald officer pleads guilty to role in deadly collision," *ABC News*, 8 May 2018, https://abcnews.go.com/US/uss-fitzgerald-officer-pleads-guilty-role-deadly-collision/story?id=55021772.

12 Zeeshan Aleem, "The WannaCry hack shows North Korea's emergence as a cyber powerhouse" *Vox* , 19 December 2017, https://www.vox.com/world/2017/12/19/16794970/wannacry-north-korea-bossert-cyberattacks.

13 Maria Korolov and Lysa Myers, "What is the cyber kill chain? Why it's not always the right approach to cyber attacks," *CSO*, 7 November 2017, https://www.csoonline.com/article/2134037/cyber-attacks-

adoption of threat management rather than risk management as more viable and effective to countering the evolving nature of cyber threats originating from advanced persistent threats (APT). APTs are a prolonged, aimed attack on a specific target with the intention to compromise their system and gain information from or about that target.[14]

Two issues notably absent within the book include the rise of cyber sovereignty in response to cyberattacks and the role of psy-ops within cyberwarfare. First, since 2011 there has been a perceptible shift within government policies towards the concept of cyber sovereignty—the notion that governments can exercise control over their digital environment.[15] This transition has accelerated since 2015 as illustrated by China's 2016 Cybersecurity Law [16] and Australia's mandatory data breach notification laws,[17] as governments sacrifice privacy rights in their attempts to track and manage cyber breaches suffered by private entities. Second, the events surrounding the 2016 US presidential election and the alarming rise of fake news indicates a perceptible shift in cyber operations employed by state and non-state actors from targeting the military and economic to the socio-political. Social media has been the main avenue of attack, with Russian bots being used to inject pernicious and false information amongst the general populace in a wider ploy to influence the political institutions and leadership of a target country,[18] and carefully crafted propaganda material supporting and inciting extremist violence being proliferated by groups such as ISIS.[19]

Summary

There Will Be Cyberwar provides a concise analysis of the implications of cybersecurity upon the US military's adoption of NCW, how its continuous difficulties in managing cyberattacks reflects upon the risks and vulnerabilities

espionage/strategic-planning-erm-the-practicality-of-the-cyber-kill-chain-approach-to-security.html

14 Pieter Amtz, "Explained: Advanced Persistent Threat (APT)," *MalwarebytesLabs*, 25 July 2016, https://blog.malwarebytes.com/cybercrime/malware/2016/07/explained-advanced-persistent-threat-apt/.

15 Sarah McKune, "An Analysis of the International Code of Conduct for Information Security" *The Citizen Lab*, 8 September 2015, https://citizenlab.ca/2015/09/international-code-of-conduct/>.

16 (中华人民共和国网络安全法) "Cybersecurity Law of the People's Republic of China" *People's Republic of China*, President of the People's Republic of China, Order No.53, 7 November 2016.

17 Paul Smith, 'New mandatory data breach notifications laws to drag Australia into cyber age' on *The Financial Review* (23 February 2018) <http://www.afr.com/technology/new-mandatory-data-breach-notifications-laws-to-drag-australia-into-cyber-age-20180222-h0whxa>.

18 Gabe O'Connor and Avie Schneider, 'How Russian Twitter Bots Pumped Out Fake News During The 2016 Election' on *NPR* (3 April 20170 <https://www.npr.org/sections/alltechconsidered/2017/04/03/522503844/how-russian-twitter-bots-pumped-out-fake-news-during-the-2016-election>.

19 Kimbra L. Fishel, 'ISIS and the Continuing Threat of Islamist Jihad: The Need for the Centrality of PSYOP' on *Moderndiplomacy* (19 April 2018) <https://moderndiplomacy.eu/2018/04/19/isis-and-the-continuing-threat-of-islamist-jihad-the-need-for-the-centrality-of-psyop/>.

faced by governments and private entities, and that the unwillingness of governments and organizations to adapt risks the inevitable occurrence of a "cyber Pearl Harbour". The intended readership of this book includes those moderately familiar with technology and politics. The book succeeds in engaging scholars of international politics through its recounting of cyber operations conducted by both state and non-state actors and its projected influence upon how these actors can be expected to interact with each other within the 21st century. However, it is also expected to intrigue cybersecurity professionals interested in military technology, IoT, public policy, and the geopolitical landscape. Steinnon's book sits as a bridge between the fields of IT and International Affairs, given its broad geopolitical predictions, perceptive insight into military affairs, and vast knowledge in relation to the nature and operation of cyber operations on a technical level. Accordingly, the book is a valued contribution to the areas of IT and International Relations given its utility as a foundational text for scholars new to the topic of cyberwarfare.