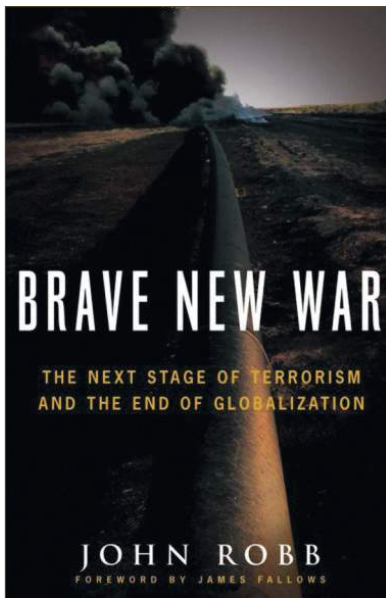




Book Review



John Robb, *Brave New War: The Next Stage of Terrorism and the End of Globalization*, New Jersey, John Wiley and Sons Inc., 2007, 208 pages.

by **Ruben Pang**

The large-scale symbolic shock of terrorism as epitomized by the September 11 attacks (9/11) has diminishing returns. Besides being difficult to repeat and sustain, the public becomes desensitized and the media pays less attention each time an attack occurs. Al-Qaeda will be hard-pressed to sustain symbolic attacks of that scale, let alone outdo 9/11. The number of people, specific skills, lead time and coordination involved is simply overwhelming.¹

Instead, the rise of smaller-scale “do-it-yourself” terrorists will be the new threat to anticipate. In recent years, these stateless terrorist groups have learned to capitalize on the technology and globalization that have been driving market changes and industries, turning the complexity and power of a developed modern economy against itself. Residing anywhere from the Middle East to London to Nigeria, they are well versed in sophisticated

technologies and thrive amidst cultural fragmentation and transnational crime.

In the *Brave New War*, John Robb cites two closely occurring Al-Qaeda attacks in 2006 as a trademark of this new terrorist approach. The first was against the Samarra mosque in Iraq which almost immediately sent the nation into civil war, as tens of thousands of Shiite Muslims took to the streets in protest. The second Al-Qaeda attack happened two days later, and was an attempt on a critical oil facility in Abqaiq which Saudi security forces foiled. If Al-Qaeda had succeeded in the attack, oil prices would have soared to over \$100 a barrel instantly.

Termed “black swans,” these rapid and unexpected attacks were planned quickly and carried out with minimal resources, yet effected near catastrophic results. As more of these attacks surface, the situation becomes one where,



according to the author, “[while] we’re busy working to protect ourselves against the previous attack, we can expect more black swans, because they are being manufactured by our foes at an increasing frequency.”²

In addition, the nature of terrorist operations has evolved. Robb asserts that the conflict in Iraq foreshadows the future challenge to global security. The insurgency in Iraq is comprised of 75 to 100 small, diverse and autonomous groups who have access to first world technologies and are able to use them effectively.³ Their strength lies in their open-sourced structure that lacks a clear centre, allowing flexibility and decision-making cycles much shorter than those of the United States (US) military. He compares this to “Microsoft finding its match in a loose self-tuning network” instead of a superpower competitor.⁴ Furthermore, as they operate like open-source communities on the internet, their actions are amplified “in a non-linear way which creates feedback loops that can dramatically escalate the impact of violence.”⁵

These connections extend to criminal networks that permeate the global economy. In Iraq, international crime is fuel for terrorist activity—Al-Qaeda’s attack on Madrid was funded through profits from the sale of the drug ecstasy and

hashish.⁶ The rapidly expanding criminal economy, valued at \$2 to \$3 trillion a year, is fuelled by a technologically enabled supply chain of anything from “human trafficking (Eastern Europe) to illicit drugs (Asia and South America), pirated goods (Southeast Asia), arms (Central Asia) and money laundering (everywhere).”⁷

The terrorist-criminal relationship is reinforced by a new terrorist strategy—systems disruption, the targeting of critical networks such as power, communication and transportation. The severance of these essential frameworks undermines the targeted state’s legitimacy, bulldozing it to failure by hindering its ability to provide basic services to citizens, eventually losing their confidence and support.⁸ This was evident in the attacks on Iraq’s oil and electricity networks since 2005.⁹ According to Robb, the attacks which cost the Iraqi government \$500 million in lost oil revenues only cost \$2000 to execute.¹⁰ It is clear that small bodies can now effect disastrous results from strategic actions, in a way unprecedented in history.

The evolution of warfare is rapid, and extends beyond Islamic terrorism. In many ways, “[the] perpetrators of this new form of warfare, however,

aren’t really terrorists, because they no longer have terror as their goal or method. A better term might be global guerrillas, because they represent a broad-based threat that far exceeds that offered by terrorists or the guerrillas of our past.”¹¹

According to Robb, successfully employing systems disruption as a method of warfare against the US could result in a situation similar to the fall of the Soviet Union—“a country driven to bankruptcy by a foe it couldn’t compete with economically.” In this scenario, defeat is experienced gradually, through an “inevitable withering away of military, economic and political power through wasting conflicts with minor foes.”¹²

For the US military, the lack of a historical guide and past experience poses a great challenge. Past encounters with guerrillas in Vietnam and beyond were considerably different from those of the present. According to Robb, “today, there are no cohesive centralized movements to fight. No wars of national liberation. Warfare is now an open-source framework of loose organizations.”¹³ Using Iraq’s insurgency as an example, Robb draws a link between global guerrillas and online retail markets through the long tail model. These separate non-state groups, ranging from external Sunni fundamentalists



to Saddam loyalists, tribal groups, Shiite fundamentalists etc. may be in competition to one another but are willing to cooperate in fighting the US through the building of a market which is mutually beneficial.¹⁴

The author warns that it is likely that unrestrained systems disruption is only the first chapter in the shape of things to come. These non-state groups have developed an organization structure which places little emphasis on centralized leadership and capitalizes on global communication networks and innovation. This effectively makes them unpredictable and very much immune to nation-state counter-pressure and containment strategies. These global guerillas wage an open-source "Wiki-War" where "the source-code of warfare is available to anyone who is interested in both modifying and extending it."¹⁵ The dynamics of open-source warfare is compared to the that of a black market bazaar's economy, where the fundamental elements are: investment in the form of international funding, outsourcing to financially motivated contractors, and crime. In Iraq, the insurgents dealing in black market oil benefit from escalating prices whenever supplies are threatened.¹⁶

This integration with international criminal networks means that every nation-state's defences will be constantly be harassed in innumerable ways. Once breached, several copycat groups will swarm the target. The bulk of Robb's writing is dedicated to the analysis of "Guerilla Entrepreneur" methods of coordination, innovation and expansion. Looking at the global oil market, he proposes the possibility of a guerrilla oil cartel profiting from bunkering and smuggling oil while sustaining continuous oil disruption through low-tech but substantial attacks, further driving up prices in a vicious cycle (pipeline disruption, kidnappings etc).¹⁷

In *Rethinking Security*, Robb's concluding chapter, emphasis is placed on the balance "between preserving the benefits of global interconnectivity and insulating against the myriad threats that can strike at us through those same connections." In his opinion, the Knee-Jerk Police State and Pre-emptive War/Nation Building are two approaches to avoid.

In the first option, centralized security under the arbitrary command of the nation-state give few benefits despite their severe drawbacks. This includes the reduction of domestic and international

moral cohesion, such as the US National Security Agency's monitoring of global telephone systems and the use of torture on suspected terrorists (for example, Abu Ghraib).¹⁸

Furthermore, a security system similar to that of the US Department of Homeland Security tends to be uniform and unresponsive, especially against the uncertainty of black swans, "failing to bounce back with new approaches [and being susceptible to] hindsight bias," as reflected in 9/11 post-mortems.¹⁹

The latter option attempts to mitigate the roots of terrorism and extremism through war and aggressive nation-building. However, Afghanistan and Iraq show that global guerillas have been able to keep these states "in a perpetual condition of failure" ever since the US invasion.²⁰ This leads to the situation where it becomes a sanctum and harbour for instabilities. Furthermore, although present threats are mostly Islamic groups, "superempowerment" through technology also means that instability will increasingly come from multiple sources.²¹

Responding to the changing landscape, Robb proposes an approach he calls Dynamic Decentralized Resilience. The future of security is held within




the notion of survival, which he defines as “the ability to dynamically mitigate and dampen system shocks.” This means restructuring current networks in a way which aids damage control through five key tenets: Thinking in Terms of Market States and Minimalist Platforms; Thinking in Terms of Platforms; Thinking in Terms of Ecosystems; Thinking in Terms of Open-Source Networks; and Thinking in Terms of Sustainability Instead of Dependence.

The notion of the market state is taken from Philip Bobbit’s *The Shield of Achilles: War, Peace, and the Course of History*, which forwards the inevitable evolution of the nation-state into a market-state, driven by economic competition and as states increasingly find the provision of welfare overwhelming. Instead, the shift towards the use of market mechanisms will create fair opportunities for all citizens. He also separately cautions the risk of economic instead of ideological conflict.

A particular obstacle for decentralized security is the culture of secrecy between local (e.g. the Terrorist Early Warning Group in Los Angeles) and federal agencies. To overcome this, he proposes thinking in terms of platform, using the internet

example of Skype as an example of a product of a platform; the online video program is built upon readily available software from Microsoft to Intel. This continuous “development of local innovation” is one of many benefits of the decentralization of security efforts which can be exponentially increased with open sourced networks as a conduit for a variety of participants.²²

Lastly, the author addresses the nature of consumption and US dependence of external sources of energy. Technology advances in sustainability should be harnessed as they cover basic to high-tech needs and can be found in geothermal heating and cooling; solar hot water and electricity; and even solar powered Internet Connection from the Green WiFi Project.²³

All in all, *Brave New War* is an assertive and accessible text on the next generation warfare that synthesizes high-tech trends with real world examples to reinforce the idea of adopting resilience and problem-solving through an open source community-sharing as a daily practice. These actions should safeguard against severe shocks on a delicate security system and encourage the perception of “community members as allies and co-developers rather than competitors.”²⁴ 

ENDNOTES

1. John Robb, *Brave New War: The Next Stage of Terrorism and the End of Globalization* (New Jersey: John Wiley and Sons Inc., 2007), viii.
2. Ibid., xiv.
3. Ibid., 4.
4. Ibid.
5. Noah Shachtman, “Inside the Brave New,” [www.wired.com](http://www.wired.com/dangerroom/2007/05/q_tell_me_a_lit/), May 2007, Warhttp://www.wired.com/dangerroom/2007/05/q_tell_me_a_lit/
6. Ibid.
7. Robb, *Brave New War*, 5.
8. Ibid.
9. Ibid.
10. Ibid.
11. Ibid., 14-15.
12. Ibid., 32.
13. Noah Shachtman, “Inside the Brave New,” [www.wired.com](http://www.wired.com/dangerroom/2007/05/q_tell_me_a_lit/), May 2007, Warhttp://www.wired.com/dangerroom/2007/05/q_tell_me_a_lit/
14. Robb, *Brave New War*, 74.
15. Ibid., 116.
16. Ibid., 119.
17. Ibid., 128.
18. Ibid., 157.
19. Ibid., 155.
20. Ibid., 160.
21. Ibid.
22. Ibid., 180.
23. Ibid., 182.
24. Ibid., 183; and Kiva Loaner, “Book Review – Brave New War,” blog entry, 8 October 2010, <http://globalsociology.com/2010/10/08/book-review-brave-new-war/>.