Non-Fiction

Financial Times

Digital destruction

MAY 10, 2013 by: Review by Shashank Joshi

Cyber War Will Not Take Place, by Thomas Rid, *Hurst, RRP£14.99, 256 pages*

In the early 20th century, the Italian general Giulio Douhet became the foremost proponent of air power with the publication of *The Command of the Air* (1921). “No longer can areas exist in which life can be lived in safety and tranquillity … ” he wrote. “On the contrary, the battlefield will be limited only by the boundaries of the nations at war, and all of their citizens will become combatants.” As the British prime minister Stanley Baldwin put it in 1932, “The bomber will always get through.”

A century on, another revolutionary and dystopian theory of warfare is coming to prominence: cyber war (http://www.ft.com/intl/indepth/cyberwarfare). This, too, anticipates a battlefield that cuts across territorial boundaries, opening up an entirely new, digital, plane of fighting, and breaches what were once sanctuaries of civilian life. Its believers foresee wars

being won from the ether; elevators plunging to the ground at the push of an adversary's button.

Yet in *Cyber War Will Not Take Place*, Thomas Rid, reader in war studies at King's College London, throws a well-timed bucket of cold water on an increasingly alarmist debate. Just as strategic bombing never fulfilled its promise, and even air power at its apogee – Kosovo in 1999, or Libya (http://www.ft.com/topics/places/Libya) two years ago – only worked with old-fashioned boots on the ground, Rid argues that the promise of cyber war is equally illusory.

Drawing on the early 19th-century Prussian theorist Carl von Clausewitz, Rid argues that war, at its core, must meet three criteria. It must be instrumental (rather than just a spasm of violence), political (rather than criminal) and at least potentially violent (else it lapses into metaphor). Rid then asserts that "not a single human being has ever been killed or hurt as a result of a code-triggered cyber attack".

What Rid does, with great skill, is to pivot the discussion away from cyber war and towards cyber weapons. Such weapons, he concedes, are capable of multiplying the effects of traditional means of war, as Israel demonstrated when it hypnotised Syrian air defences before flattening a half-built nuclear reactor in 2007.

But worms and viruses carry no explosive payload. “Code-caused destruction,” Rid argues, “is parasitic on the target.” Even one of the most potent such weapons, Stuxnet (http://www.ft.com/cms/s/0/cbf707d2-c737-11df-aeb1-00144feab49a.html), a computer worm created, it is assumed, by the US and Israel (http://next.ft.com/content/08b8b06e-ac04-11e1-923a-00144feabdc0) and unleashed on Iran’s nuclear programme, could only compel a limited number of Iranian centrifuges to shake themselves into breaking.

Nonetheless, the contrarian title of Rid’s book belies one of its most important insights: that cyber weapons, though limited in the physical destruction they can cause and difficult to wield with precision, can achieve certain political effects with far less violence than was once necessary.

This is truest of sabotage. It once demanded that individuals took grave personal risk (consider the wartime saboteur) and did lasting damage to hardware (such as machinery in a factory). Compare that to the August 2012 cyber attack on Saudi Arabia’s national oil company (http://www.ft.com/cms/s/0/5f313ab6-42da-11e2-a4e4-00144feabdc0.html), which wiped the hard drives of 30,000 computers. This principle also holds for espionage, now indelibly associated with the Chinese theft of commercial secrets, and subversion, whether for good (mobilising against dictators) or bad (radicalisation

by jihadists). This, “the retreat of violence”, is the crux of Rid’s argument.

Rid concludes by exploring a powerful idea: small cyber attacks are hard to attribute and easy to repeat. Big ones – think Stuxnet – are easier to attribute but harder to repeat. They are therefore harder to use as instruments of coercion. Rid infers from this that cyberspace favours the defence.

I am not so sure. The world is full of examples of sporadic attacks used as coercive tools, nearly always attributed, directly or indirectly, to a state – but with some uncertainty and usually after a lag. Think of North Korea sinking a South Korean ship, or Pakistan sponsoring terrorist groups directed at India. Cyber attacks may be incapable of inflicting corporeal harm – “more ethical than an airstrike” – and they may not constitute war, as it is classically defined. Yet that does not mean they cannot slot comfortably into a pseudo-guerrilla role: as hyped as air power, while less violent and more versatile.

Shashank Joshi is a research fellow of the Royal United Services Institute

---