S. RAJARATNAM SCHOOL
OF INTERNATIONAL STUDIES
A Graduate School of Nanyang Technological University

RSIS COMMENTARIES

No. 119/2013 dated 28 June 2013

Information Warfare 3.0: Weapons of Mass Effectiveness

By Michael Raska

Synopsis

The information revolution over the past two decades has led to significant changes in security threats, vulnerabilities, character and conduct of warfare. The next wave of future information warfare may evolve further, with the development of 'Weapons of Mass Effectiveness' (WMEs).

Commentary

THROUGHOUT HISTORY, the control and use of information and intelligence has played a vital role in diplomatic relations as well as combat, primarily as a 'first line of defence' in reducing the possibility of strategic surprise. In 500 B.C., Sun Tzu noted that 'all warfare is based on deception' – a thought that inspires intelligence tradecraft to this day as 'there are friendly nations, but not friendly intelligence services'.

With the increasing political, military, and socio-economic challenges of globalisation amplified by growing strategic uncertainties and threats in nearly every security domain, intelligence agencies worldwide have been developing increasingly sophisticated ways of collecting intelligence. These are based on innovative information and cyber strategies and capabilities to safeguard their freedom of action and to provide political decision-makers with timely actionable intelligence.

'Three Waves' of Information Revolution

In the process, they have learned to take advantage of global information and communications interdependence. This essentially enables unprecedented intelligence collection opportunities: the ability to operate quickly, against adversaries located far away without risking the lives of intelligence operatives; the ability to act in secret, while minimising the exposure and risks of counterattack; the ability to access communications systems, banking and finance, logistics and transportation systems, national databases; the ability to penetrate and disrupt specific targets using low entrance threshold in technology, knowledge, and capital.

The 'digital' transformation of intelligence has evolved in parallel with the global information revolution and related conceptual developments of information and cyber-warfare in the military domain over the past two decades. The first IW wave began in the early 1990s when the United States military experimented with 'defensive information operations' vis-à-vis Iraq during the Gulf War, which gave the US military an edge in battlefield intelligence, targeting, and command and control.

From mid-1990s, a second wave emerged with the considerable developments in computer and communications technologies, which sparked a conceptual debate on future conflicts in the information age. While the information warfare debate was still confined primarily to the military domain, particularly with emerging concepts such as ‘cyberwars’ in both offensive and defensive modes, its scope gradually included intelligence-based warfare, economic warfare, cyber-warfare, and hacker warfare.

Indeed, one of the most influential concepts became the idea of ‘netwars’ – information-related conflict at the grand strategic level between nations and societies, involving various forms of networks in economic, political, and social domains.

With each technological wave, the global diffusion of information technologies has accelerated, resulting in unprecedented global connectivity options that provided individuals, groups, and governments with unparalleled capabilities to deny, disrupt, deceive, and destroy information systems and environment. Currently, we are in the third wave of ‘integrated information operations’ that include electronic warfare, computer network operations, psychological operations, military deception, intelligence and cyber-espionage.

Future of Information Warfare

From limited hacker incursions to attacks by politically-motivated hacktivists, corporate and military intelligence agencies, organised crime and terrorist groups, to advanced information warfare programs of nation-states, cyber and information warfare is about exploiting and protecting information in diverse survival contests. For many, however, information warfare is still an enigma.

This is due to the continuously evolving and multidimensional character of IW that absorbs advancing information and communications technologies, while blurring distinctions between its civil and military domains, types of conflict, targets, modes and magnitude of attacks.

Indeed, today’s information revolution focuses on types of information conflict that empowers individuals and groups such as WikiLeaks or Anonymous to organise, collaborate, and network in new ways in order to force political and social change. In their view, it is no longer possible for governments, corporations, militaries, or other traditionally powerful organisations and institutions to monopolise information or to significantly restrict access to information.

The recently exposed global surveillance programmes run by the U.S. National Security Agency (NSA) and British Government Communications Headquarters (GCHQ) coupled with the debate of the cyber-espionage capabilities of NATO, China and Russia, shows the new direction for information conflicts.

In particular, the next wave of information warfare may be propelled by the idea of Weapons of Mass Effectiveness or WMEs. These will combine select elements of cyber and information warfare, including mass-media information denial, disruption, destruction and manipulation campaigns, confrontations in cyberspace, attacks on computerised systems, cyber-attacks on physical infrastructure systems, cyber-espionage, electronic warfare, and perception management.

WMEs will essentially integrate conflicts for information, through information, against information in a new form of information warfare between individuals, states, and non-state networks. WMEs will target traditional governmental bureaucracies, intelligence agencies, and military organisations that will become increasingly vulnerable in their ability to control the flow of information.

Michael Raska is a Research Fellow at the Institute of Defence and Strategic Studies (IDSS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University in Singapore.