ELSEVIER

Journal of International Management
11 (2005) 563–580

THE FOX SCHOOL of Business and Management
TEMPLE UNIVERSITY

Information and communications technologies, strategic asymmetry and national security

Nir Kshetri *

Bryan School of Business and Economics, University of North Carolina at Greensboro, Bryan Building, Room: 368, P.O. Box 26165, Greensboro, NC 27402-6165, United States

Received 14 December 2004; accepted 14 September 2005

Abstract

In the history of warfare, there are a number of examples of strategic uses of asymmetric technologies. Consistent with history and theory, individuals, organizations and nations have spotted opportunities to employ information and communications technologies to gain and exploit asymmetric advantages and to counter asymmetric weaknesses. This article discusses various asymmetries associated with institutions, nations and organizations that influence the ICT-national security nexus. Regulative, normative and cognitive institutions in a country provide various mechanisms that affect the nature of positive and negative asymmetries. Nations and organizations also differ in terms of their capability to assimilate ICT tools to gain positive asymmetries and deal with vulnerabilities of negative asymmetries. Integrative approaches that combine policy and technological measures at various levels are likely to make the world more secure.

Keywords: Strategic asymmetry; Information and communication technologies; National security; Institutions; Cyber attacks

1. Introduction

Information and communications technologies (ICTs) play a critical role in the national security game (e.g., English, 2005; Metz, 2001; Zhou, 2005). The vulnerability to threat as well as the capability to strategically deploy ICTs vary across entities. The characteristics of organizations, nations and institutions superimpose in a unique interaction with ICTs' nature that influence the ICT-security nexus.

* Tel.: +1 336 334 4530; fax: +1 336 334 4141.
E-mail address: nbkshetr@uncg.edu.

1075-4253/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.intman.2005.09.010

Table 1
Explanation of major terms used in the paper

Term	Explanation
Encryption technologies[a]	These technologies transform text or data into a coded form that is close to impossible to read without the key to decode the message. This scrambling of the message is done by using a mathematical formula.
ICTs[b]	These include telecommunications as well as digital technologies such as telephony, cable, satellite, radio, computers, information networks and software.
Negative asymmetry[c]	A difference an adversary is likely to use to exploit a weakness or vulnerability.
National security	"Measures taken by a state to ensure its survival and safety". "Includes the deterrence of attack, from within and without, as well as the protection and well-being of citizens".[d]
Positive asymmetry[c]	Capitalizing on differences to gain an advantage.
Steganography[e]	A technique that allows hiding messages within pictures, music, and other media. Steganography can be used with or without encryption. It is, however, of limited use without encryption.
Symmetric advantage[c]	The advantage that can result from matching the opponent in terms of strategic resources.
Strategic asymmetry[c]	Employing "some sort of differences to gain an advantage over an adversary". It could be real as well as perceived.
The Gramm–Leach–Bliley Act[f]	The Gramm–Leach–Bliley Act of 1999 went into effect in July 2002. It mandates that all financial institutions establish procedures for protecting personal information, including the protection of discarded information. Financial penalties and civil suits may result from the inadvertent disclosure of personal information.
The USA Patriot Act[g]	The USA Patriot Act was enacted on October 26, 2001 to expand the intelligence gathering and surveillance powers of law enforcement and national security agencies.

[a] See http://www.loansnap.com/security.htm.
[b] See http://www.google.com/url?sa=X&start=0&oi=define&q=http://www.cyber.law.harvard.edu/readinessguide/glossary.html.
[c] Metz (2001), Metz and Johnson (2001).
[d] See http://www.en.wikipedia.org/wiki/National_security.
[e] Maney (2001), Hernandez et al. (2004).
[f] http://www.allshredservices.com/faq/grammleachbliley.htm.
[g] Young (2004).

The focus of this paper is on asymmetry (see Table 1 for definitions of terms) associated with ICTs from the perspective of national security. Asymmetry created by ICTs (more broadly: technologies) is among six forms of asymmetry identified by Metz and Johnson (2001). Nations and organizations can exploit asymmetric advantages by strategically employing ICTs in war against enemies (e.g., cyber attacks) as well as by using ICTs in facilitating other functions contributing to attack and defense such as communications, detection of threats from enemies, gathering intelligence, etc. The Internet as well as non-Internet ICTs such as wireless telephony, satellite TV, satellite phones and supercomputers can be employed in the management of asymmetries (see Table 2).

In the history of warfare, there are several examples[1] of strategic uses of asymmetric technologies (Metz, 2001) that have provided "a decisive advantage over an opponent in

[1] The Maxim Machine-Gun adopted by the British Army in 1889 is a good example of an asymmetric technology. A Maxim gun could fire 500 rounds per minute—equivalent to that of 100 rifles at that time. In the 1893–1994 Matabele war, 50 British soldiers with just four Maxim guns fought of 5000 Matabele warriors (see http://www.spartacus.schoolnet.co.uk/FWWmaximgun.htm). Similarly, asymmetric technologies used by the U.S. Army include, cruise missiles, laser-guided bombs, satellite reconnaissance systems, high altitude reconnaissance aircraft, and unmanned aerial vehicles (Rosenberger, 2005).