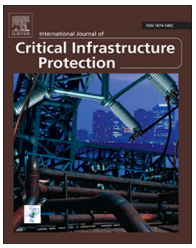
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



The anatomy of a cyber power

*Jill Rowland, Mason Rice, Sujeet Shenoi**

Tandy School of Computer Science, University of Tulsa, Tulsa, Oklahoma 74104, USA

ARTICLE INFO

Article history:
Received 28 August 2013
Accepted 19 January 2014
Available online 23 January 2014

Keywords:
Cyberpower
Cyber power
Anatomy
Characteristics

ABSTRACT

Cyberspace, the ever-expanding manifestation of the pervasive information and communications infrastructure, is a rich environment for the projection of power and influence. Entities of all types – nation-states, corporations, terrorist and criminal organizations, and non-profit groups – are embedding critical aspects of their operations in cyberspace hoping to reap the benefits offered by the domain. Cyberspace is an equalizer. It offers all actors speed and reach, anonymity and protection, and the ability to create and participate in virtual economies and wield cyber weapons, all with a low buy-in cost. This drastically alters the power equation. The gap between major powers and lesser powers is shrinking; non-state actors could become cyber powers. This paper attempts to clarify the important notions of cyberpower and cyber power. It considers nation-states as well as non-state actors, and articulates the essential components and characteristics required to acquire and maintain cyberpower.

1. Introduction

Scholars have offered myriad definitions of power. Organski [28] defines power as the ability of an entity (usually a state) to influence the behavior of other entities according to its goals. Nye [25] describes power as the ability of an entity to influence another entity to achieve desired outcomes, and the ability to make the entity do something it would not otherwise do.

Keohane and Nye [14] identify two types of power – hard power and soft power. Hard power is the ability of an entity to use threats or rewards to get other entities to do what they otherwise would not do. Soft power is the ability of an entity to obtain desired outcomes because other entities want the same outcomes – it is the ability to achieve goals through attraction rather than coercion.

Power requires resources. Nolte [24] sees national power as control over resources, principally military resources. Other resources include wealth, time, political capital [9], geographical size, population and economic strength measured by gross domestic product (GDP) [15]. Nye [25] identifies population, territory, natural resources, economic size, military forces and political stability as the resources required for national power. Organski [28] lists several similar components, including geography, resources, population, economic development, political development and national morale. However, Wight and colleagues [42] give credit to "less tangible elements like administrative and financial efficiency, education and technological skill, and above all moral cohesion."

A definitive answer to "What is Power?" is by no means simple. However, it is clear that the two overarching themes of power are resources and influence. Indeed, resources and influence crystallize into four elements – diplomatic power, informational power, military power and economic power – that have come to be known as the DIME model of national power as articulated during the Carter and Reagan administrations [22,23].

The five domains of power – land, sea, air, space and cyberspace – enable the generation and acquisition of resources and influence. The five domains are also vital to project

*Corresponding author.
E-mail address: sujeet@utulsa.edu (S. Shenoi).

1874-5482/$ - see front matter © 2014 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.ijcip.2014.01.001

economic power and influence. The first powers were land based. As technology advanced, great maritime powers developed. Air superiority during World War II was vital to victory. Control over air and space was pivotal during the Cold War. Now, cyberspace has come into existence; it is the new frontier for wielding the instruments of power – diplomacy, information, military and economics. The pervasiveness of cyberspace supports near instantaneous action in all five domains of human power – land, sea, air, space and cyberspace.

Entities of all types – states, corporations, terrorist and criminal organizations, and non-profit groups – are embedding their operations in cyberspace. The ability to pursue their agendas and acquire power in cyberspace is such an appealing possibility that entities will be more engaged in cyberspace than ever before.

There are several reasons for the transition to cyberspace. Nye [27] attributes the shift to the proliferation of information in cyberspace predicted by Moore's Law, and to the power diffusion that takes place in cyberspace because of information proliferation. Nye recognizes that many diverse entities will participate and, indeed, wield power, in cyberspace. However, Nye maintains that states will be the dominant actors, although the wide availability of information will allow other entities to rise in power status. Nye also describes some of the other advantages that cyberspace offers, notably the low barriers and costs of entry. Cyberspace provides anonymity that is not available in the other domains of power, and movement in cyberspace occurs faster and cheaper than in any other domain. Asymmetric vulnerabilities in cyberspace also give smaller cyber entities an advantage over larger cyber entities.

This paper attempts to clarify the important notions of cyberpower and cyber power. It considers nation-states as well as non-state actors, and articulates the essential components and characteristics required to acquire and maintain cyberpower.

2. Cyberspace and cyber entities

The term "cyberspace" was first used in 1984 by William Gibson in his novel *Neuromancer* [8]. Gibson described cyberspace as a "consensual hallucination" – a world into which people physically connected and explored with disembodied consciousnesses. The word cyberspace comes from "cybernetics," coined by Wiener [41] in 1949 to describe the communication process that occurs between machines, and between humans and machines [30]. In the early 1990s, John Perry Barlow appropriated the word cyberspace to express the modern concept of the relationship between computers and telecommunications networks [39]. This paper draws on Barlow's version of cyberspace in defining a cyber entity as one that straddles the virtual and physical worlds.

More specifically, this paper considers cyberspace to be the "consciousness" created within the pervasive information and communications infrastructure. This virtual world requires components from the physical world in order to exist and flourish. These components include hardware, software, data and people, all of which require resources (e.g., electricity, buildings, telecommunications and food and drink). In other words, cyberspace is built from and uses resources from all five domains – land, sea, air, space and cyberspace.

Cyber entities have already emerged in a number of domains. Google, which was founded in 1998, is one of the most successful companies to leverage a virtual (cyber) presence to generate real earnings. Sixteen years later, it is the preeminent cyber corporation. While Google earns the vast majority of its revenue in cyberspace, it has created diverse business units, several of them in the physical world.

Facebook is a more recent incarnation of a corporation rooted in cyberspace. It earns substantial revenue, but of more consequence in this discussion about power, Facebook has hundreds of millions of users, many of them passionately devoted to social networking.

The Internet Underground is another cyber (albeit criminal) entity with an infrastructure, economy, financial system, shareholders and customers, and considerable muscle within and outside cyberspace [37,38]. Wikileaks is yet another type of cyber entity, transnational in its scope, with many adherents devoted to its ideology. Its active support of Edward Snowden, the NSA leaker, as he evades U.S. justice [11], demonstrates that it can defy an angry superpower and persist.

The era of cyber entities has only just begun. Science fiction abounds with tales of pure cyber entities, as in the *Matrix* series. Such entities may well exist in the future. However, this paper focuses on cyber entities that straddle the virtual and physical worlds. They will be more advanced evolutionary versions of Google, Facebook, the Internet Underground and Wikileaks. They will be corporations, non-profits, criminal and terrorist organizations, social, religious and activist groups, perhaps even cyber states.

3. Components of a cyber entity

National power requires resources and the ability to project influence. However, non-state actors can also possess significant resources and project power locally, and sometimes regionally or globally. A non-state actor is a non-sovereign entity that does not "own" its domains of operation like a nation-state. Typically, non-state actors operate in national, multinational or extra-national jurisdictions. Non-state entities have a long history; they include the Knights Templar, the East India Company, the Barbary Pirates and the Catholic Church. These entities are becoming more common now because of globalization and cyberspace [21].

A cyber entity could be a state or non-state actor. Non-state cyber entities include corporations, criminal and terrorist organizations, non-profits as well as social, religious and activist groups. As mentioned above, cyber entities necessarily operate in cyberspace and in the physical world. They leverage resources from the five domains of power (land, sea, air, space and cyberspace) to conduct activities along one or more of the four dimensions of power (diplomacy, information, military and economics) to promote their agendas. In general, cyber entities have three components: an ideology, a body politic and an infrastructure.