Chapter XXXVIII
Digital Convergence and Cybersecurity Policy

Anthony W. Buenger, Jr.
National Defense University, USA

INTRODUCTION

Digital convergence constitutes the full realization of the Information Age and provides the foundation to link cultural, personal, business, governmental, and economic affairs into a rapidly expanding global digital world called cyberspace. However, this linking of people around the globe is challenging the government to actively work with private industry to ensure its critical infrastructures and associated information is adequately protected. The purpose of this chapter is to explain how digital convergence is affecting the public sector and the need for a cybersecurity policy that includes the active involvement of both the public and private sectors.

Digital convergence has made incredible inroads thanks to rapidly developing technologies such as the ubiquitous Internet, seemingly endless bandwidth (including wireless), and rapid advances in computer processing power that are all responsible for the processing, transporting, and storing of digital information throughout cyberspace. Moreover, these technologies have brought about the collision of three colossal industrial segments within the private sector—(a) computing, (b) consumer electronics, and (c) telecommunications providers—and are providing a multitude of compatible services via various digital devices (Figure 1). Without a doubt, the explosion of digital convergence has produced a flourishing multimedia, multidevice, and multitasking environment (Baker & Green, 2004). A significant impact of a converged society is the empowerment of individuals (consumers) and organizations to collaborate and compete on a global scale. Most importantly, however, these highly mobile and perpetually connected consumers are putting information at a greater risk as they have access to this information outside of its traditionally protected network boundaries in an environment where this information is increasingly vital to the nation's critical infrastructure assets. The government must be able to effectively secure the information flowing throughout cyberspace.

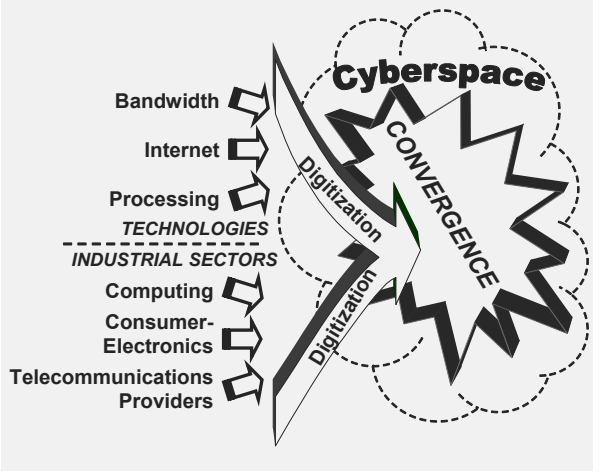
BACKGROUND

The idea of digital convergence is not new, but has grown exponentially over the last 15 to 20 years as digitized capabilities became widely available, affordable, and usable. A significant milestone on the path to digital convergence can be traced back to the late 1970s when Steve Jobs and Bill Gates gave up their analog typewriters for the digitized

personal computer (PC). Around the same time in 1978, James Martin in his book *The Wired Society* envisioned the integration of mobile, wireless phones, the Internet, small powerful PCs, e-mail, telecommuting, and portable digital devices into a technical savvy society (Martin, 1978). Martin's visionary concept is truly amazing considering that PC and software gurus like Steve Jobs and Bill Gates may still have been pecking away at their analog typewriters in 1978.

Since then, mobile, digital, multimedia devices have invaded the home, office, and academic environments. The maturation of integrated circuit-board technology allowed for the rapid development of smaller computing devices. PC processing power became more powerful and easier to produce, manufacturing costs dropped, availability increased, and consumer costs subsequently dropped to commodity levels. The ubiquitous presence of the Internet, along with robust bandwidth and mobile devices, now links consumers, employees, and corporations in cyberspace, enabling them to work outside the traditional workplace. The term cyberspace, although overused and not always understood, simply means being connected to the digital global world. The virtual world of cyberspace, where everyone has a feeling of connectedness, and fostered via the Internet and collaborative capabilities, provides ubiquitous online capabilities to allow employees to work virtually from anywhere and at anytime.

Figure 1. Digital convergence environment



Rapidly advancing digital-based technologies continue to pave the way for integrated multimedia on a single portable device. Moreover, with these devices, individuals are empowered to collaborate and compete globally on their own behalf more than ever before (Friedman, 2005). Cyberspace is no longer a mutually exclusive computer-led, television-led, Internet-led, or cell-phone-led race to the finish line. Up until very recently, cell phones and personal digital assistants (PDAs) have led the convergence push by incorporating digital cameras, Web browsers, and radio receivers into conveniently small devices. However, the playing field is muddled as these multimedia capabilities are incorporated into digital platforms that can seamlessly collaborate with each other any time of day or night. As a result, individuals have endless access to the information they need, whether at home or in the workplace.

IMPACTS

Digital convergence has far-reaching implications and is directly tied to the security of the nation's critical infrastructures. Furthermore, digital convergence has changed the nature of the industry and how consumers use information that is accessible 24 hours per day (Huston, 1998). However, the dependence on digital information from both the private and public sectors makes it especially critical to protect this information as it is processed, stored, and transported throughout cyberspace. In particular, the private development of the Internet has accelerated the security risks to the nation's critical infrastructure assets, including the transportation, oil, power, energy, health, and information infrastructures. The information infrastructure, in which the Internet is one element and along with digitized capabilities provides the foundation for cyberspace, is traditionally privately owned and operated. In other words, both the public and private sectors depend on a reliable Internet for their mission-critical and vital life functions, and both have responsibility to ensure that cyberspace is a safe and trusted environment (George Mason University, 2006). Both sectors