Chapter 93
The Winds of Change in World Politics and the Impact on Cyber Stability

Virginia Greiman
Boston University, USA

ABSTRACT

One of the greatest geopolitical challenges in the 21st century will be competing for the control of cyberspace, the 5th domain of cyberwarfare after land, sea, air, and space, and the major economic challenge of the time. With the advancement of artificial intelligence, the Internet of Things, autonomous vehicles, and unmanned drones, this challenge becomes even greater. This article explores through empirical evidence the interaction among the three powers that shape cyber intelligence and international security: globalism, regionalism, and nationalism. Recently, world politics has created a sense of urgency concerning the new world order and what that means for cyber security and the domain of cyberspace. With the recent cyberattacks targeting the American political system, the Foreign Ministry of the Czech Republic, the government of Croatia, and the 2017 attacks on the cyber systems operated by the Ukrainian government, there is concern about the stability of global connectedness and the potential for diminution of global boundaries. The concern about global stability raises the question of who controls cyberspace and who is accountable when things go wrong. The aim of the article is to advance a conceptualization for cyber governance frameworks for better control of cyber security by governments, intergovernmental organizations, and the private sector.

INTRODUCTION

Defending cyberspace in a changing technological world must be understood, in its domestic and international dimensions in order to prepare ourselves for uncertain world events. The trends created by technology and political changes complicate our ability to understand the core political dynamics of cyberspace, but at their center are three significant issues that will shape the governance of cybersecurity.

DOI: 10.4018/978-1-7998-7705-9.ch093

These are questions about the evolving nature of sovereignty, the role of globalization and regionalism, and the impact of rising nationalism.

One of the important goals of cyberspace control by the United States is the expansion of American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet. The 2018 U.S. strategy on cyberspace has focused on protecting America's national security and promoting the prosperity of the American people as top priorities. The strategy demonstrates the President's commitment to strengthening America's cybersecurity capabilities and securing America from cyber threats. The new strategy is a call to action for all Americans and its companies to take the necessary steps to enhance national cybersecurity to continue to lead the world in securing a prosperous cyber future (WH, 2018).

The U.S. Military perspective on cyber war has been described this way:

If you're asking me if I think we're at war, I think I'd say yes …We're at war right now in cyberspace. We've been at war for maybe a decade. They're pouring oil over the castle walls every day (Seffers, 2019, Kinetic Weapons Remain a Priority as Cyber War Rages, 1), --Gen Robert Neller, Commandant, USMC, 21 Feb 2019

On October 12, 2018, the Secretary of the Navy directed a comprehensive cybersecurity review following several significant compromises of classified and sensitive information (DON, 2019). The task was to examine the Department of the Navy (DON) current cyberspace governance structures to assess if they are optimally focused, organized, and resourced to prevent or mitigate future incidents. It is this war before the war, and its consequential impact on outcomes to be, that is the existential threat to national security (DON, 2019). This cyber war has been ongoing for some time. The threat is long past the emergent or developing stage. By some estimates, economic espionage is costing the US $400B annually and has cost approximately $1.2 trillion since 2015 (NBAR, 2017). The winds of change are happening now but are the governance structures that will oversee this change prepared to adapt to a more nationalistic approach to cyberspace? Further, in the current struggle for global influence and dominance, US economic strength has been materially eroded by years of tolerated, massive commercial Intellectual Property (IP) theft (NBAR, 2017).

This research attempts to map out systematically global, national and regional efforts to control cyber space by understanding the relationship of these three powers in terms of convergence and divergence and areas for harmonization and cooperation. This analysis builds on published research, organizational frameworks, and interviews with professionals and experts engaged in the development of cyber initiatives. The goal is to offer empirically grounded frameworks for thinking about the dynamic relationships between the three major cyber powers and how they are influenced by changes in the national and international political environments. The main contribution of the research is to enrich existing theory on the interrelationships among the cyber powers to enable policy makers and cyber professionals to better prepare for the evolving landscape of cyber threats.

In the networked world we continue to ponder the meaning of cyberspace, globalization, nationalism, regionalism, and transnationalism. As reflected in the literature, globalization is a force that has shaped world politics and the move toward economic, social, and legal integration (Drucker, 1997; Fawcett and Hurrell, 1996). Globalization often synonymous with transnationalism, because it refers to cross border activity, is viewed in large part as a positive movement that enhances the benefits and opportunities for individuals, corporations, and governments worldwide (IMF, 2016). Globalization refers