June 2018

The Importance of Information in International Relations

Njabulo Bruce Khumalo
National University of Science and Technology - Zimbabwe, njabulobass@gmail.com

Miniyothabo Baloyi
Zimbabwe National Defence University, baloyimini@yahoo.com

Introduction

The impact of information on international relations is highlighted by Finn (nd) who posits that most international relations experts who in the past dismissed the information revolution as a force for real political change are now changing their minds. Information has always been an important part of international relations as Westcott (2008:18) suggests that reliable information and informed analysis have always been at the heart of foreign policy making. Webster (2006) further notes that information is a distinguishing feature of the modern world. Economies were once built on industry and conquest, but information has become a driving factor for economies. Local, national and international news agencies circulate information and images between countries and form relationships between people from the local level to the international level (BoydBarrett and Rantanen, 2001: 127). To put it in the words of Bollier (2003) information, technology, and institutional flexibility have gained importance in international relations as power in the global information society depends less on territory, military power, and natural resources. Furthermore, Wriston (1997:176) avers that in international relations, the competition for the best information has replaced the competition for the best farmland or coal fields.

The advent of the internet has further bolstered the role of information in international relations as it has made access to information much easier than it was before. The possibility for information to travel across the world in virtually no time, and the increasing availability of high-speed internet has dramatically altered the general dynamics in politics and global affairs (McGlinchey, 2017:44). Information has become a valuable part of politics and international relations. Rothkopf (1998:326) suggests that "the realpolitik of the new era is cyberpolitik, in which the actors are no longer just states, and raw power can be countered or fortified by information power. Furthermore, Malec (2003:46) opines that information is the best security weapon by nature and its significance rises together with the rapid development of technology, in terms of both processing and collecting (computers), and dissemination (media). To Deakin (2003) electronic communications and processing technologies have accelerated the role of information which has since become the very essence and manifestation of competition, conflict and war.

Information has emerged as a security issue influencing all aspects of human life and the ability to control information flows as a function necessary to preserve national sovereignty and boost national security (Agnew and Corbrige, 1995: Malec, 2003). When offensive information operations are used by national and government entities (state actors) against other countries, be they state or non-state targets, the detection and defensive operations can be complex and impinge on often sensitive international relations (Hearn, Williams and Mahncke, 2010:7). This study sought to establish the importance of information and information communication technologies in international relations.

Problem Statement

Information has become a very important resource in international relations. However, some governments and their leaders have not fully comprehended the importance of information in international relations. This ignorance has led to the low attention given to information security, privacy and being prone to cyber-attacks, and the failure to exploit information and information communications technologies to further their national interests in international relations. This study sought to establish the role played by information and information communication technologies in shaping international relations.

Purpose of the Study

This study sought to establish the role played by information and information communication technologies in shaping international relations. The specific objectives of the study were to:

i. Establish the role played by information in shaping international relations;
ii. Determine how the internet has affected international relations; and
iii. Establish how nations/states are using information to further their interests.

Methodology

This study applied a literature review as its methodology. The authors conducted a literature search on Google with the aim of retrieving articles, journal papers, theses, dissertations, reports and other documents which discussed information in international relations. Search terms used included information in international relations, international relations, and the internet in international relations and information communication technologies in global affairs. However, these researchers concur with Vaishnav, Choucri, and Clark (2013) who acknowledge that there is very little literature on cyber international relations. The researchers realised that there is scarcity of literature which discuss the role of information and information technology in international relations. The researchers therefore, had to search for literature which discussed international relations which had sections, subsections or paragraphs devoted to information in international relations.

The Nexus between Information and International Relations

Information is crucial to the emerging phenomenon of global localism (otherwise known as globalisation) whereby international and local issues and interests are connected and managed (Webster, 2006:97). Bollier (2003:1-2) notes that as the velocity of information increases and the types of publicly available information diversify, the very architecture of international relations is changing dramatically. State and sub-state officials from a number of countries work together to share information with each other, develop harmonized guidelines and best practices, and reduce friction associated with globalization (Bach and Newman, 2010). Furthermore, Deakin (2003) is of the view that an increasing flow of information between countries eliminates the uncertainties about each other's intentions and increases transparency, reducing mutual suspicion as well as the risk of misperception. Webster (2006:97) posits that information flows are a requisite of a globalised economy, particularly those financial and service networks which tie together and support dispersed activities.

Nations around the globe are developing network intelligence gathering capabilities in an attempt to gain privileged intelligence, especially for military information (Hearn, Williams, Mahncke, 2010). Quality information can be applied to improvements in fire power and lethality, manoeuvrability, command and control, interoperability of forces, and precision application of forces. (Deakin, 2003). When offensive information operations are used by national and government entities (state actors) against other countries, be they state or non-state targets, the detection and defensive operations can be complex and impinge on often sensitive international relations (Hearns, Willaims and Mahncke, 2016). Simmons (2011) stresses that the Information Age has also offered governments a number of possible ways to weaken their opponents. Russia is able to use democracy against democracies and the freedom of information to inject disinformation into various target groups under the label of freedom of speech (Cižik, 2017). Information warfare blurs the border between peace and war and between fact and fiction (Cižik, 2017:6). Information warfare and propaganda has the power to influence whole states and alliances without direct military involvement, so it can be considered as a powerful tool of geopolitics (Cižik, 2017).

The unequal access to information reinforces the political and cultural dominance of the North (Sawyyer, 2004:214). Through the export of ICT products, the "information powers" dominate information in underdeveloped nations and thereby threaten their economic security (Kshetri, 2014:20). The majority of societies face a real threat from the unequal access to current information and modern knowledge and this leads to unequal development and exchange in international trade, widening the development gaps between the information-rich and information poor among and within countries and regions (Sawyyer, 2004:214).

Kalathil (2002) highlights that the information revolution has helped create a multicentric, fragmented world, in which the concept of sovereignty has retreated in favour of an a-territorial, neo-medieval system of overlapping jurisdictions and loyalties. According to Nye (2004:53) increased information flows through the media have caused the loss of government's traditional control over information in relation to politics. Furthermore, as with economic interdependency, communication drives the creation of forums in which societal interests are articulated on a trans-national rather than on a national basis (Deakin, 2003). Westcott (2008) further points out that the audience now for any public information is always global; and diasporas, as well as foreign ministries, are capable of taking collective political action at a global level. To Cižik (2017:2) globalization and the information era allowed information warfare to gain new dimension, and states, coalitions and alliances became more interconnected and interdependent and therefore it is easier to influence more than one state at the time. One's state action will influence the decision-making and actions taken of other state and vice versa (Cižik, 2017:2).

The Power of the Internet in International Relations

The internet and other information technologies are no longer a peripheral force in the conduct of world affairs but a powerful engine for change (Bollier, 2003:38). The strategic significance of the internet lies in the fact that it has become an effective tool that breaks national boundaries, communicates information worldwide, and influences international and domestic affairs (Liberation Army Daily, 2011). Greenberg, Goodman and Hoo (1998) postulate that the ability of signals to travel across international networks and affect systems in distant countries conflicts with the longstanding principle of national, territorial sovereignty. To Hearn, Williams and Mahncke (2010:9) the space on the internet is a media environment that encompasses the ‘world stage’ of politics and it provides the space in which international relations are played out and therefore, one of the ways that international relations are played out is via information warfare. The power of the internet in shaping international relations is projected by (Hearn, Williams and Mahncke (2010:10) who point out that it (the internet) plays a role in the visualisation and articulation of international relations both officially and unofficially. Moreover, the internet and all other networked information technologies influence the global politics, including democratization and terrorism (Seib, 2008). Countries like China and Russia have raised concern over the fact that the cyber could threaten the political legitimacy of nations (Sasore, 2016). Arquilla and Ronfeldt (1996) suggest that some scholars also suggest that information technology may contribute to the development of new forms of social organization, along with new forms of conflict.

The ease of accessing information and communicating it at a global stage has affected diplomacy. Bollier (2003:5) quotes Madeleine Albright who highlighted that “the large numbers of information systems make diplomacy much harder to carry on, because the information comes in very fast and you have to make decisions much faster than you might under previous circumstances”. While new technologies can facilitate the rapid spread of ideas, this can have both positive and negative consequences. The easy manipulation of information and sources and the risk of viral dissemination without verification can propagate misinformation (the Independent Commission on Multilateralism and the International Peace Institute, 2016:7). The advent of the Internet has opened new opportunities of virtually unlimited manipulation with information: commonly referred to as propaganda” (Cižik, 2015). Many decisions are based on incomplete information and taken under time pressure, for example, economic sanctions may turn a latent conflict into a crisis (Pfetsch, Rohloff, 2000: 382).

Mallik (2016) posit that ICTs can combine world-wide information and knowledge for promoting universal good and addressing common concerns of future global society. Technologies such as e-mails, virtual and online conferencing at international negotiations, also make it possible for delegations to communicate in real-time with the home office for information on official positions, or for advice on formulating responses to unanticipated issues, and reactive diplomacy (Mallik, 2016:16). The use of IT tools has become the norm at international negotiations, facilitating speedy communication and more comprehensive information gathering and analysis (Mallik, 2016:17).

Westcott (2008:3) avers that the internet has played a crucial role in levelling the playing field across the globe, enabling anyone, anywhere, to have access to the same information, to connect to and do business direct with each other. The international flow of information has grown at an extraordinarily rapid rate, thus saturating the capabilities of a state to monitor closely what information goes in and what goes out of its territory (Eriksson and Giacomello, 2006). 2006). Hearn, Williams and Mahncke (2010) posits that this allows for the participation of groups outside of governments to play a part in foreign relations at an unofficial level. Powers that were once the monopoly of nation-states participation in international politics, control of transnational communications, and credibility as sources of accurate information are now being exercised by a much wider array of players (Bollier, 2003). The internet can also facilitate the spread and uptake of radical ideologies; the so-called Islamic State uses social media to recruit people from around the world (The Independent Commission on Multilateralism, 2016).

The Use of Use of Information Communications Technology in International Relations

Countries are using ICTs and information to further their interests. The internet represents a space in which international relations are contested in terms of cyber-attacks and information warfare (Hearn, Williams and Mahncke, 2010). Moore (2013) notes that countries frequently use cyber technology to conduct passive information gathering and offensive operations on other states. In international relations, even small or economically less developed countries may use the cyberspace to inflict harm to bigger and economically more developed countries (Kshetri, 2014). It is often reported in the South Korean and western media that North Korea has carried out hack attacks on South Korea and as such, the relationship between North Korea and the international community is in part played out and visualised on the internet (Hearn, Williams and Mahncke, 2010:7). Moreover, the internet is being used for different agendas as the United States of America has been accused of supporting internet freedom in order to intervene in the politics of other countries while also serving to consolidate its cyber-hegemony (Sheng, 2010). The United States loses $300 billion per year as a result of industrial and economic espionage conducted on line and some 122 countries conduct such espionage.

Sasore (2016:1) also highlights that on several different occasions, the United States has accused the People's Republic of China of hacking into or compromising information systems belonging to the United States or United States entities. Lewis (2015) also points out that China's military is responsible for most hacking against the United States and some of this is the normal political-military espionage that the United States itself is well-known for. Furthermore, some countries and their military units are said to hack to make money as espionage is a source of private income when they steal commercial secrets and sell them to companies for cash or favors (Lewis 2015). Xiaokun (2012) opines that China has been the target of serious cyberattacks from the United States and such attacks from the US have been as grave as the ones the US claims China has conducted.

Sasore (2016) further notes that some countries use their military and other units to hack into corporate computer systems of other countries to obtain proprietary intellectual property that could help advance their economy. Chinese military members hacked into the corporate computer systems of several United States companies and obtained proprietary intellectual property that could help advance China's economy (Sasore, 2016:1). The *Washington Post* reported that Chinese hackers were allegedly responsible for hacking the information systems of the United States Office of Personnel Management (OPM) in early 2015, which resulted in the release of personal information belonging to thousands of United States Government employees (Nakashima 2015).In the Brexit case, the inaccurate statement of Boris Johnson, that the UK sends Brussels £350m a week can be considered as incorrect information that was massively spread via social media and one of the reasons why UK citizens voted to leave the European Union (Lythgoe and Dixon, 2016). ICTs are also being used by the Russian Federation to influence decision-making on the European level and in the same time, it is using elements of hybrid warfare to challenge NATO (Cižik, 2017:6).

Information is being used by countries around the world for different reasons. Coalson (2016) highlights that Russia identifies threats such as the expansion of the use of ' information-psychological influences' by foreign intelligence services aimed at the destabilization of various regions of the world, including Russia. The day before the Ukraine presidential election, Ukraine's Security Service discovered a virus in the systems of the Central Election Commission designed to compromise data collected on the results of the election, revealing how close Russian hackers had come to sabotaging the results (Maurer and Janz (2014).

The Emergence of Information Warfare or Cyber- Attacks

Mallik (2016:34) highlights that technology has changed the nature of warfare from visible large-scale military action and violence to subtle, invisible yet decisive capabilities for crippling the enemy's information environment in a war-like situation. The use of information in warlike fashion is highlighted by Deakin (2003:49) who posits that in 1996, the USA publicly declared information superiority in its Joint Vision 2010 as the key-enabling element of twenty-first century warfare. Furthermore, since Russian annexation of Crimea, in March 2014, the international community experiences massive use of information warfare in international affairs and informational warfare has become one of the most challenging issues (Cižik, 2017:1). The potential for information warfare is vast and is of concern to all nations and national security defence (Hearn, Williams and Mahncke, 2010:10). Coban (2016) highlighted that faster and easily accessible information within global media had triggered the information wars among the states which have changed power politics. Information warfare became very dangerous tool in international affairs, which can fulfil one's own political and military goals without need to send an army into foreign countries or without any significant investments into hard power military capabilities (Cižik, 2017:1). Waller (1995) also opines that information warfare could usher in an era of largely bloodless conflict; battle would occur in cyberspace, where information warriors would be able to disable important enemy command and control or civilian infrastructure systems with little, if any, loss of life.

Information warfare is composed of "six pre-existing subareas", which are: "operational security, electronic warfare (EW), psychological operations (PSYOPs), deception, physical attack on information processes, and information attack on informational processes' (Cižik, 2017:1). Tucker (1999) argues that information warfare could be used to disable computer networks, paralyzing communications, transportation, power systems, and industrial enterprises. The use of terms such as information "warfare" and "electronic Pearl Harbour convey a special meaning: that which is digital by nature has, nonetheless, physical consequences comparable to those of conventional war (Eriksson and Giacomello, 2006). On an international level, information warfare is used to create realities, to undermine trust of citizens into their political elites and democratic institutions, to undermine trust of states to each other, to create chaos and to invoke fear among citizens (Cižik, 2016). The shared nature of cyberspace is increasingly becoming associated with war-like terms such as "attack," "offensive," "defensive," "intelligence," and "operations." In this environment, illicit activities go beyond traditional military players, and combat-related actions can be carried out by civilian and state actors with increasingly advanced means and nefarious intent (Sasore, 2016:1).

It is often reported in the South Korean and western media that North Korea has carried out hack attacks on South Korea and as such, the relationship between North Korea and the international community is in part played out and visualised on the internet (Hearn, Williams and Mahncke, 2010:9). The USA too is believed to be developing plans for cyber warfare attacks (Hearn, Williams and Mahncke, 2010:9). The information and network struggle, including its extreme forms, such as information-psychological warfare and netwars, are means the state [Russia] uses to achieve its goals in international, regional and domestic politics and also to gain a geopolitical advantage (Darczewska, 2014). Deibert and Rohozinski (2009) note that Chinese cyber-espionage is a major global concern and that Chinese authorities have made it clear that they consider cyberspace a strategic domain, one which helps redress the military imbalance between China and the rest of the world (particularly the United States)".

Dempsey (2014:26) stresses that all nations on the face of the planet always conduct intelligence operations in all domains, but China's particular niche in cyber has been theft and intellectual property. North Korea is often reported in the media, to have trained computer hackers to launch cyber-attacks against other countries such as the United States of America (USA) and South Korea (Security Focus, 2004). Maurer and Janz (2014) dozens of computers in the Ukrainian prime minister's office and several embassies outside of Ukraine had been infected with malicious software called Snake capable of extracting sensitive information. While the operators of the Snake malware were located in the same time zone as Moscow, and Russian text was found in its code, the evidence that the malware originated in Russia is circumstantial (Maurer and Janz (2014). In 2003, a security breach created numerous leaks of sensitive information from U.S. Department of Defence computers, which occurred over several months (Wilson, 2008). The Department has acknowledged that the majority of such incidents collectively referred to as "Titan Rain" were orchestrated by China as a method of cyber-espionage (Wilson, 2008). The US Department of Defence admitted that it suffered one of its worst cyber-espionage leaks in March 2011, when foreign hackers gained access to over 24,000 Pentagon files (Shanker and Bumiller, 2011).

Consequences of Cyber-attacks and Information Security Breaches

There are a number of consequences of cyber-attacks or information wars which cannot be fully exhausted in this study. the United Nations Group of Governmental Experts' (GGE) Code of Conduct proposed that states should agree not to use "information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies" (2014:324). Cyber-attacks or security breaches expose security weaknesses in information security protection plan of countries and also places citizens at risk of hostile foreign governments (Sasore, 2016).Furthermore, cyber-attacks can potentially damage economies of countries which are attacked (Hearns, Williams and Mahncke, 2016). Maurer and Janz (2014) highlight that NATO member states officially declared that cyber-attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Estonia, a highly technological country, was brought to its knees by a series of attacks in 2007 that initiated in Russia and greatly disrupted Estonia's banking systems (Moore 2013:227). Westcott (2008:14) noted that private information, when made public, may have a swifter and more profound impact on the conduct of world affairs. Information leaks may lead to the permanent damage to the reputation of countries, weakening their moral authority in the world and fuelling attacks and wars (Westcott, 2008:14).

Conclusion

Information and information communication technologies have become a central and critical aspect in international relations. Information is at the heart of political, economic and military development hence the move by countries around the world to grapple for it. This study concluded that information is greatly shaping international relations, and that the internet has further made information accessible and central to world affairs. Furthermore, this study concluded that information is becoming more valuable for economic and political spaces than natural resources such as mines, farmland among other things. These researchers also concluded that the unequal access to information in international relations is the major reason behind the emergence of rich and developed countries and poor ones which have no access to information. The internet has also made access to information a possibility and in the process giving rise to information wars and cyber-attacks. Some countries which were militarily inferior to world powers have found the cyber to offer them leverage as they use it to attack great powers or even gain political and economic mileage. Furthermore, wars are being conducted on the cyber in the same manner they were or are being conducted in combat. This study therefore concluded that, information has become a very key element in international relations and it therefore needs to be managed meticulously to protect a country's intellectual property, citizens, security and health inter alia. Information and or cyber security has become a critical issue as nations are being exposed to more and more attacks and espionage.

References

Agnew, J. and Corbrige, S. 1995. *Mastering space: Hegemony, territory and international political economy*. London: Routledge.

Arquilla, J and Ronfeldt, D. 1996. *The Advent of Netwar.*

Bach, D, and Abraham L. N. 2010. Trans-governmental networks and domestic policy convergence: Evidence from insider trading regulation *International Organization*. *Summer* 64(3):505-28.

Bollier, D. 2003. *The rise of netpolitik: How the internet is changing international politics and diplomacy*. The Aspen Institute: Washington.

Boyt-Barret and Rantanen, T. 2001. News Agency Foreign Correspondents" in Tunstall, J. (ed.) *Media Occupations and Professions,* Oxford University Press.

Camilleri, J. A. and Falk, J. 1992. *The end of sovereignty? The politics of a shrinking and fragmenting world.* Aldershot: Edward Elgar.

Cižik, T. 2017. *Information warfare as a geopolitical tool. Centre for European and North* Atlantic Affairs.

Cižik, Tomáš. 2016. Russian Information Warfare – Security Threat not only for Visegrad Countries". *Nemzeti Érdek (National Interest Journal), Volume 17*. Századvég Alapitvány (in Hugarian).

Cižik, Tomáš. 2016. Information warfare – Europe's new security threat". *CENAA Policy Papers, 5.* Centre for European and North Atlantic Affairs. (Online) Available at: http://cenaa.org/en/new-policypaper-information-warfare-europes-new-security-threat/. (Accessed 22 September 2017).

Cižik, Tomáš. 2015. Implications for Security and Defence Cooperation of the Nordic-Baltic Region Following the Annexation of Crimea by Russian Federation". In Róbert Ondrejcsák and Grygoryi Perepelytsia (eds.). *Ukraine, Central Europe and the Future of European Security*. Bratislava: Centre for European and North Atlantic Affairs. pp. 66-87.

Coalson, R. 2016. New Kremlin Information-Security Doctrine Calls For ‘Managing’ Internet in Russia”. December 6. *Radio Free Europe – Radio Liberty*. Available at: http://www.rferl.org/a/russiainformaiton-security-internet-freedomeconcerns/28159130.html.

Coban, F. 2016. The role of the media in international relations: From the CNN effect to the Al –Jazeera effect. *Journal of International Relations and Foreign Policy*, 4(2): 45-61.

Darczewska, J. 2014. The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study. *Centre for Eastern Studies (OSW). (Online)* Available at: https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf (Accessed 22 September 2017).

Deakin, R. L. 2003. Economic information warfare: Analysis of the relationship between the protection of financial information infrastructure and Australia’s national security. Master Thesis: Queensland of University Technology.

Eriksson, J. and Giacomello, G. 2006. The information revolution, security, and international relations: (IR) relevant theory? *International Political Science Review / Revue internationale de science politique*, 27(3): 221-244.

Finn, E. nd. *International relations in a changing world: A new diplomacy*.

Greenberg, Goodman and Hoo. 1998. *Information Warfare and International Law. United States National Defence University Press:* Washington DC.

Hearn, K., Williams, P. A. H. and Mahncke,R. J. 2010. International relations and cyber-attacks: Official and unofficial discourse. Paper published in the Proceedings of the 11th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia,30th November - 2nd December 2010.

Independent Commission on Multilateralism and the International Peace Institute. 2016. The Impact of New Technologies on Peace, Security, and Development: Independent Commission on Multilateralism.

Kalathil, S. 2002. Community and Communalism in the Information Age,” *Brown Journal of World Affairs*, 9(1). (Online) Available at http://www.ceip.org (Accessed 22 September 2017).

Kello, L. 2013. The meaning of the cyber revolution: Perils to theory and statecraft. *International Security,* 38(2): 7-40.

Kshetri, N. 2014. Cybersecurity and international relations: The U.S. engagement with China and Russia. Prepared for FLACSO-ISA 2014, University of Buenos Aires, School of Economics, Buenos Aires, Argentina, July 23-25.

Lewis, J. A. 2015. Moving Forward with the Obama-Xi Cybersecurity Agreement.” Center for Strategic and International Studies. https://www.csis.org/analysis/moving forwardobama-xi-cybersecurity-agreement (Accessed 22 September 2017).

Liberation Army Daily. 2011. Experts Discuss Prospects of ‘Cyber Defence’ and National Defence, January 4, 2011.

Lythoe, Luke and Dixon, Hugo. 2016. “EU-bashing stories are misleading voters – here are eight of the most toxic tales”. *The Guardian.* May 19. Available at: https://www.theguardian.com/commentisfree/2016/may/19/inaccurate-pro-brexit-infacts-investigationmedia-reports-eu-referendum. (Accessed 22 September 2017).

Malec, M. 2003. *Security perception: Within and beyond the traditional approach. Masters Dissertation: Naval* Postgraduate School: Monterey, California.

Mallik, A. 2016. Role of technology in international affairs. Institute for Defence Studies and Analyses, New Delhi.

Maurer, T. and Janz, S. 2014. *The Russia-Ukraine conflict: Cyber and information warfare in a regional context.* International Relations and Security Network (ISN): Zurich.

McGlinchey, S. 2017. *International relations*. E-International Relations Publishers: Bristol.

Moore, S. 2013. Cyber attacks and the beginnings of an international cyber treaty. *North Carolina Journal of International Law and Commercial* Regulation 39(1): 223-57.

Nakashima, Ellen. 2015. Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say.” *Washington Post*, July 9, 2015. (Online) Available at: https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearancesystem-affected-21-5-million-people-federal-authorities-say/ (Accessed 23 September 2017).

Nye, J. 2004. *Soft power: Means to Success in World Politics*, USA: Public Affairs

Pfetsch, F. R. and Rohloff, C. 2000. *National and International Conflicts, 1945-1995,* New Empirical and Theoretical Approaches. Routledge.

Rothkopf, D in “Cyberpolitik: The Changing Nature of Power in the Information Age. *Journal of International Affairs*, 51(2): 325–59.

Sasore, A. 2016. The 2015 United States-China Cyber Security Agreement and Its Impact on International Cyber Conduct. Webster University. Master of Arts.

Sawyyer, A. 2004. African universities and the challenge of research capacity development. JHEA/RESA, 2(1): 211–240.

Simmons, Beth A. 2011. International Studies in the Global Information Age**.** *International Studies Quarterly* 55(3):589-99.

Tucker, J. B. 1999. Asymmetric Warfare, http://forum.ra.utk.edu/1999summer/asymmetric.html (Accessed 22 September 2017).

Seib, P. 2008. *The Al Jazeera Effect: How the new global media are reshaping world politics.* Potomac Books Inc.

Shanker, T. and Bumiller, E. 2011. *Hackers Gained Access to Sensitive Military Files*, N.Y. TIMES, at A6, July 15, 2011.

Sheng, Z. 2010. To defend 'freedom', or to defend hegemony?" *People's Daily*, January 26, 2010.

Vaishnav, C., Nazli, C. and David, C. 2013. Cyber International Relations as an Integrated System. *Environment Systems and Decisions,* 33(4): 561-76.

Waller, D. 1995. Onward cyber soldiers, Time, Aug. 21, 1995, at 37

Webster, F. 2006. Theories of the information society.(3rd edition). Routledge: New York

Westcott, N. 2008. Digital diplomacy: The impact of the internet on international relations. *Oxford Internet Institute, Research Report 16, July 2008.*

Wilson, C. 2008. Botnets,cybercrime, amd cyber terrorism: Vulnerabilities and policy issues for congress 12.

Wriston, W, B. 1997. Bits, bytes, and diplomacy. Foreign Affairs, Vol. 76, No. 5, September-October 1997, p. 178.5.

Xiaokun, L. 2012. *China is victim of hacking attacks.* Available at http://english.peopledaily.com.cn/90883/8271052.html (Accessed 22 September 2017).