A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War

Rika Isnarti[*]
rika_isnarti@fisip.unand.ac.id

Abstract

Cyberwar can be considered as one of phenomena in International Relations. However, recently, there are not many literature about International Relations theory talking about cyber war or cyberspace generally. The phenomena of cyberspace is matter to International Relations as it involved sovereignty, state interactions and other elements in International Relations theory. On the other hand, cyber space blurs many concept in International Relations such as sovereignty is borderless in the realms of cyber space. Therefore, this articles analyses three perspectives in International Relations in analyzing cyber war. It explains what cyber war in context of International Relations, how three theories in International Relations with their elements analyses actors and interaction in cyber space. Finally, it found that Neorealism is the most adequate theory among other two theories in analyzing cyber war.

Keywords: cyber war, neorealism, liberalism, constructivism

[*]Staf Pengajar Jurusan Ilmu Hubungan Internasional, Universitas Andalas

Introduction

This paper utilises three traditions in International Relations, neorealism, liberalism, and constructivism, in an analysis of cyberwar. The paper consists of three parts. The first part explains cyberwar; the second examines how neorealism, liberalism, and constructivism can be applied to an analysis of cyberwar; and the last part identifies which of these theories is most adequate to analyse cyberwar.

Cyberwar can be considered an International Relations problem. However, there appears to be little International Relations literature on the subject.[155] Though some literatures do discuss the technology and policy related to cyber security. Dunn Cavelty suggests that the phenomena in cyberspace are a matter for International Relations as they involve sovereignty, state actors, state relations and other elements.[156] Cyberspace blurs the concept of sovereignty as it is borderless. States can act in the cyber realm without territorial limitation. Actors in cyberspace are not only states but also private companies that build e-systems which also suffer from cyberattack. There are also hackers, sometimes from the military and in other times from civilian, who conduct cyberattacks. In terms of state relations, the transnational, unidentifiable character of cyber space and conflict makes it hard to determine who is a friend and who is an enemy. Further, both strong and weak states can effectively conduct cyber-attacks.

Theories in International Relations could explain cyberwar differently. Although many theories in International Relations discuss war and national security, they analyse them differently. Neorealism is a state centric theory and security is the main concern. Thus, neorealism can explain much about state behaviour in the conduct of cyber war. Liberalism is a tradition which promotes cooperation in the international system, with other actors apart from the state seen as very important. So, perhaps Liberalism can better explain how to solve the problem of cyberwar.

Through cooperation amongst various state and non-state actors. Constructivism sees international phenomena such as states as socially constructed, not given. This theory can be used to explain why cyberwar occurs, its conduct, and the various processes and actors involved. Each of the three theories explains cyberwar from a different point of view, identifying and analyzing different

[155] Maximilian_Mayer, Mariana_Carpes, & Ruth_Knoblich. (2014). the Global Politics of Science and Technology: An Introduction *the Global Politics of Science and Technology - Vol. 1 Concepts from International Relations and Other Disciplines* (pp. 1-38): Springer. P. 4

[156] Cavelty, M. D. (2010). Cyberwar. In G. Kassimeris & J. Buckley (Eds.), *the Ashgate Research Companion to Modern Warfare* (pp. 123-144). Aldershot: Ashgate. p.127

structures, units, actors and processes. Therefore, it is important to first explain what cyberwar is.

What Is Cyberwar?

Cyberwar was first associated only with military action.[157] Cyber war complemented physical or kinetic war. To win a military conflict it is important to secure one's own military information but also to be able to attack an enemy's military information systems. However, due to the development of cyber space, cyber war is not only limited to physical military strategy.[158] It is used widely to attack enemy computer systems in order to destroy or disturb the systems of nation-state, particularly digital infrastructure such as transportation, telecommunication, gas pipeline controls, and nuclear power controls. Clarke and Nauke define Cyber war as "Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption".[159]

There are many different types of activity in cyberspace, such as cyber vandalism, cyber campaigns, and cybercrime. Not all actions can be categorized as cyberwar. Thus, an attack on computer systems should only be called cyberwar if it is carried out with warlike intentions.[160] We need to note that cyberwar is related to kinetic war or physical conflict.[161] Cyberwar will always be part of the larger kinetic war or conflict, whether to start kinetic war or conduct kinetic war.

There are four phenomena in cyber insecurity they are cybercrime refers to an action aiming to steal money from networks. Hactivism refers to an action to steal information for political purposes so they can spread to public, such as wikileaks, anynomous and so on. Cyber espionage is associated with an action to steal information particularly from company or from university regarding research and development and send the information to other companies so they can take advantages or get the information without having to pay much money to do research by their own and the last one is

[157] Cavelty, M. D. (2013). Cyber security. In A. Collins (Ed.), *Contemporary Security Studies* (3 ed., pp. 361-378): OUP Oxford. P. 369

[158] Choucri, N. (2012). *Cyber politics in International Relations*. Massachusetts: MIT Press. P.3

[159] Clarke, R. A., & Knake, R. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*: HarperCollins.p.6

[160] Cavelty, M. D. (2010). Cyberwar. p.14

There are four phenomena in cyber insecurity they are cybercrime refers to an action aiming to steal money from networks. Hactivism refers to an action to steal information for political purposes so they can spread to public, such as wikileaks, anynomous and so on. Cyber espionage is associated with an action to steal information particularly from company or from university regarding research and development and send the information to other companies so they can take advantages or get the information without having to pay much money to do research by their own and the last one is cyber war.

See further, Greathouse, C. B. (2013). Cyberwar and strategic thought: Do the Classic Theorists Still Matter? In J. F. Kremer & B. Müller (Eds.), *Cyberspace and International Relations: Theory, Prospects and Challenges* (pp. 21-40). Berlin: Springer. P. 23-26

[161] Libicki, M. C. (2014). Why Cyber War Will Not and Should Not Have Its Grand Strategist. *Strategic Studies Quarterly, 8*(1), 23-39. P.36

cyber war. For example in 2008 when Russian's tanks entered Georgia, there was cyber-attack on Georgian networks. Its government website and banking system cannot be accessed as usual.[162]

There are some characteristics of cyberwar that make it different from kinetic war. First cyber war is much cheaper than kinetic war.[163] To conduct a cyber-attack do not need specialist or sophisticated tools. Anyone who can connect to computers and networks can conduct cyberwar. A state involved in cyber war does not have to buy and rely upon sophisticated military tools such as tanks, missiles, canons, or modern fighters. The state only needs cyber warriors, computers, and networks. Therefore, a state with a weak economy can also become involved in cyber war. Consequently the identity of major cyber actors is unpredictable. Participation in cyber war does not depend on state economic power. Any state can become a cyber-power.

Second, cyberwar does not necessarily involve the loss of many human lives on the battlefield, or the conquest of and territory.[164] The objective of cyber war is to cause disruption of state networks systems, particularly important digital infrastructures vital to human life. Third, in term of actors, cyberwar can be conducted not only by state military and security organisations, but also by civilians with cyber 'know how'.[165] Almost anybody can be a cyber-warrior or cyber invader. It is hard to make sure who the invaders are, whether military or civilian. A state that suffers from a cyberattack may not be certain of the identity of the attacker.

In addition, Barlow argues that the elusive nature of cyber war presents a number of new challenges regarding unidentifiable actions.[166] For example, in 2009, someone, probably under Chinese state instruction, hacked a US defence contractor's computer and stole the plans for the new U.S F-35 plane. However, Barlow argues that many cyber-attacks such as this may have unpredictable and mixed motives, including espionage, acts of war, or commercial piracy.[167] Many of the actors cannot be recognized. There was only an assumption that the hackers were

[162] Nazario, J. (2009). Politically motivated of Denial of service attacks. In C. Czosseck & K. Geers (Eds.), *the Virtual Battlefield: Perspectives on Cyber Warfare* (pp. 163-181). Virginia: Ios Press.p. 167

[163] Kassab, H. S. (2013). In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare. In J. F. Kremer & B. Müller (Eds.), *Cyberspace and International Relations: Theory, Prospects and Challenges* (pp. 59-76). Berlin: Springer. P. 69

[164] Rueter, N. C. (2011). *The Cybersecurity Dilemma.* (Master of Arts), Duke University, Durham. P. 37

[165] Choucri, N., & Goldsmith, D. (2012). Lost in cyberspace: Harnessing the Internet, international relations, and global security. *Bulletin of the Atomic Scientists, 68*(2), 70-77. P.71

[166] Barlow, J. (2010). Cyber War and U.S. Policy: Part I, Neo-neorealism. *The journal of education, community and values, 10*(5), 1-11. P.3

[167] Barlow, J. (2010). Cyber War and U.S. Policy: Part I, Neo-neorealism. P.7

from China because the Internet Protocol address was traced to China.[168] However, the actor could be non-Chinese. Another example occurred on 4 July 2009, when U.S and South Korean government websites, the New York Exchange, the Pentagon, and the blue house (executive office and official residence of the President of the Republic of South Korea) were attacked by 'denial of service' attacks.[169] Some U.S cyber experts found that the IP address was from China, but they were not sure whether the state of China did the attacks.[170] However, they did find that a coded message was sent by a North Korean agent, which contained simple set of instructions to start attacking a list of U.S. and South Korean government and corporate websites.[171] The U.S concluded that, North Korea sent their cyber warriors to China and conducted the cyber-attack, or that there was a possibility that North Korea cooperated with China to conduct the attack. This demonstrates the difficulties in identifying cyber attackers.

Cyber war is a new type of war. This phenomenon introduces new and different processes, actors and units, different to those associated with conventional kinetic war. Many International Relations theories talk much about war but not about cyber war. As this phenomenon is part of international relations it is important to look at how International Relations theories interpret and analyse cyber war.

Neorealism and Cyber Warfare

Neorealism is a theory in International Relations focusing on the structure of the international system and its growing interdependence. This tradition explains states behaviour in the international system including how states seek relative or absolute power.[172] Further, neorealism is also a state centric paradigm. Neorealists such as Kenneth Waltz argue that the international system is in a state of anarchy.[173] There is no higher authority than states. Thus, there is no guarantee that a state will not attack another state. Fear and uncertainty drive states to maximize their military capability, economic capability, and other powers.[174] This theory is known as offensive

[168] Gorman, S., Cole, A., & Dreazen, Y. (2009, April 21, 2009). Computer Spies Breach Fighter-Jet Project. Retrieved 1 June 2015, 2015, from http://www.wsj.com/articles/SB124027491029837401

[169] Weaver, M. (2009, 8 July 2009). Cyber attackers target South Korea and US. Retrieved 1 June 2015, 2015, from http://www.theguardian.com/world/2009/jul/08/south-korea-cyber-attack

[170] CNN. (2009, 8 July 2009). U.S. government sites among those hit by cyberattack. Retrieved 1 June, 2015, from http://edition.cnn.com/2009/TECH/07/08/government.hacking/index.html?iref=24hours

[171] Clarke, R. A., & Knake, R. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*: HarperCollins.p.18

[172] Jørgensen, K. E. (2010). *International Relations Theory: A New Introduction*. New York: Palgrave Macmillan. P.85

[173] Jørgensen, K. E. (2010). *International Relations Theory: A New Introduction* .p.84

[174] Dunne, T., Kurki, M., & Smith, S. (2013). *International Relations Theories*. Oxford: OUP Oxford. P. 77-78

neorealism.[175] On the other hand, Walt and other defensive neorealists argue that if states gain too much power, the international system will punish them in term there would be another states try to be balance with them.

The defensive neorealist 'offence-defence balance' concept can be used to understand why cyberwar happens, and to explain state behaviour in response to cyberwar. Dunne explains the offence-defence balance as follows:

> Offence defence balance indicates how easy or difficult it is to conquer territory or defeat a defender in battle. If the balance favours the defender, conquest is difficult and war is therefore unlikely. The reserve is the case if the balance favours the offence.[176]

In addition, Jervis argues that technology is one of the major determinants in the offence-defence balance, and that less costly and more effective technology tends to cause insecurity, making wars more likely.[23] More precisely, cyberwar is more likely to happen if offensive gains are likely, given the defender's weak position in the offence-defence configuration. Therefore, as in physical war, cyber war is likely to happen when attack is made easier by weak defences in cyber systems.

There are also several reasons why offensive action is more likely to happen in cyberwar. First, from the cost point of view, it is much cheaper to design cyber offensive weapons than create cyber defensive weapons. For example according to Singer and Friedman, the cost of cyber offense in the U.S military is three times less than the cost of cyber defence because offensive cyber capability directly translates to power, whereas defensive cyber capability can only be measured by more or less complex and fuzzy risk assessments.[24] To create cyber weapons, you only need software and capable cyber invaders. You do not need hardware because you can attack and destroy an enemy's hardware systems. However, to create cyber defence you need good firewalls, antivirus software, and complex software and hardware maintained by capable cyber warriors.

Second, Richard argues that cyber defence will fail in cyber warfare.[25] The problem is how to avoid attacks on all national networks. Perhaps a country's military can defend a state's computer systems. However, in cyber warfare the intruder does not only attack state digital infrastructure but also private. digital infrastructure such as banking systems. Further, much infrastructure today is

[175] Dunne, T., Kurki, M., & Smith, S. (2013). *International Relations Theories*. p. 77

[176] Dunne, T., Kurki, M., & Smith, S. (2013). *International Relations Theories*. Oxford: OUP Oxford.p.355

operated by private companies, including power grids and transportations. How are they going to build cyber defence as strong as the military cyber defence? Further, Richard also gives examples of some countries that can do cyber defence in simple ways.[26] First, Russia, where the state controls and operates the internet networks in the whole country, and second China, which does filter everything that enters its cyber space. However, other countries have weaker cyber defence capability.

Another offensive advantage in cyberwar is it is difficult for the victim to identify the attacker. Cyberattacks can be conducted anywhere, even from outside the country that sponsored it. In addition, as cyber war is designed to support physical conflict, a potential attacker is more likely to do attack as fewer lives would be lost.

However, there are some limitations of the neorealist 'offence-defence balance' concept when analysing cyberwar. First neorealism tends to focus on states or great powers as the primary players in the international system.[27] However, this is makes it difficult to identify ***who is*** the great power in cyber space. Every state has their own cyber capability, including small states, weak economic states, and weak military power states. This does not mean they are weak power in cyber space. For example North Korea has no cyber space but has cyber warriors and cyber capability.[28]

Second, neorealism is used to analyse the structure of the international system: the distribution of power, and changing power configurations. However, as in the first point, it is difficult to predict such matters in cyber space and cyber warfare. In the physical world we can measure with some accuracy a state's power, but not so in cyber space. For example, the U.S is a great military and economic power but in cyber space the U.S is a country which tends to face frequent cyberattacks.[29] In kinetic war, it is easier to measure a state's capabilities, but in cyberwar it would be difficult. So, neorealism fails to adequately explain the configuration of power in the cyber international systems. It is hard to say whether some states are more or less powerful than others. How we can map the international cyber power? There are so many actors in cyber space, not just states.

Liberalism and Cyber Warfare

Liberalism is a theory that emphasizes there are various actors in the international system beyond the state. Liberalism is concerned about how to promote peace and stability amongst states and other actors through cooperation and consensus.[30] Like neorealism, this tradition views states as the major actors in the

international system, however, the role of other units, such as organizations, individuals, and social movement groups need to be recognised.

Liberalists view war as most likely to occur between militaristic and undemocratic governments pursuing their interests and extending their powers. [31] Burchill argues that war is a way for the governments to increase their control over citizens, and raise taxes.[32] On the other hand, democratic countries have little interest in conflict with each other. Rawls claims that liberal democracies are less likely to engage in war, unless they need to defend themselves, or do so to protect human rights or vulnerable liberal states. [33] For example, in 1998, the U.S joined a humanitarian intervention during the Kosovo war. At the time, the U.S and NATO used cyberattacks as one of their war strategies. U.S hackers hacked Serbian air defence systems, and spied on the email accounts of Serbian elites.[34]

In term of ideology, cyberwar is like kinetic war. States may go to war because they have different ideologies. It is rare for democratic countries to attack each other in cyberspace. Most cyber-attacks by democratic states are against states with a different ideology, such as Syria, China, Russia, and Iraq, all cyberattacked by the U.S. as part of a kinetic war strategy. However, cybercrime, hactivism, and cyber espionage is conducted between democratic countries. For example, in May 2015, an Australian hacked the U.S army and Microsoft stealing U.S army software for helicopter simulation, and intellectual property related to Microsoft's new Xbox.35 Australia and the U.S are both liberal democracies, yet this 'cyber espionage' occurred.

In terms of actors, there are many powerful actors in cyber space. Ericksson and Guacomello state that;

> Cyber-threats weaken the sovereignty and security of the state. Non-state actors are becoming even more numerous and powerful because of the information revolution.[36]

Therefore, governments alone cannot secure cyber space. There are individuals, terrorist groups, and other activist groups that are all capable of cyberattack. Further, private sectors also own and operate networks. For example private companies own and operate internet service providers but do not have the same security capacity as states. Although states would have the technological capability, it would not be enough to protect all private companies from cyberattack. As a result, liberals believe government alone cannot secure cyberspace. There should be international

state-corporate cooperation to secure cyberspace.

In order to secure cyber space, there are many international agreements both bilateral and regional/multilateral designed to create cyber peace. For example in May 2015 Russia and China signed a cyber-security pact with both countries agreeing not to conduct cyberattacks against each other.[37]At the regional/multilateral level, there is the Council of Europe Convention on Cybercrime which aims to protect the signatories from cybercrime and computer fraud. However, to date there is no comprehensive multilateral global agreement regarding cyber security, cyberattack, or cyber war.[38] There is no global consensus or cooperation on the matter.

Like neorealists, liberals agree that the international system is characterised by anarchy.[39] Therefore, it can be difficult to achieve cooperation amongst state actors. Liberals, like neorealists, acknowledge that there are some significant barriers to international cooperation.[40] For example, there may be a lack of information about another state's capabilities and intentions, creating a fear that the other state will cheat, despite signing an international agreement. Therefore, despite liberal optimism about international cooperation, we cannot be certain about whether international agreements and institutions can effectively deal with cyber security and war. Liberalism does not provide sufficient information or argument about how liberal norms and institutions will run effectively in this field.

Constructivism and Cyber Warfare

Constructivism is a theory that views the field of international relations as a social construct. While neorealism analyses what is, and liberalism prescribes what ought to be, constructivism analyses how things have been socially constructed, and how such constructs can in turn be changed. While neorealism and liberalism accept the notion of a state of anarchy, where peace and stability are secured through the balance of power or liberal institutionalism, constructivists, see anarchy as a social construct, not a given state.[41]

There are some key concepts from constructivism that can be used to analyse cyber war. Constructivists see the international system as a condition created by how states or actors see themselves and others, and this can shape their interactions. There is a correlation between identities, interests, and interactions between those different identities, particularly state elites.[42] Identity is a core concept in constructivism. Identity relates to how people see themselves, and these identities shape their preferences and

interests. Identities cannot be presumed, or taken for granted. The formation of identities and interests is a social process, the product of people's interactions with society and other elites and peoples. Communication amongst elites is important in understanding and reshaping the identity and interests of others. Through communication, interaction and networking elites may learn about one another and come to see others as friends rather than enemies.[43] In order to interact effectively with each other in the international system there needs to be recognised norms or standards of behaviour. Norms are constructed by actors who have strong ideas about what is appropriate behaviour for states.[44] Therefore, there are guidelines in the international system for actors to follow. In addition, constructivism also emphasizes culture. Constructivists refer to culture as a set of practices that give some sort of meaning to shared experiences and actions.[45] Culture is important to construct the values and rules that inform identity. States previous experiences will shape their identity.

To understand cyberwar through the constructivist lens, unlike neorealists or liberals, we are not going to analyse what states or other actors may need to do to deal with cyberwar. We are going to analyse how cyberwar is socially constructed. The advances in technology have led to the development of cyberspace, such that cyberspace can be used to threaten national and human security. Thus, cyber space and cyber war have widened the concept of security.

Previously, security in international relations was only identified with how to secure physical spaces, such as land, sea, air and space, for national security purposes. However, the focus of security has in part shifted to include cyber space as this area can also be used to harm the state. There has been a shift in the value of 'spaces'. Cyberspace facilitates cyberwar leading to fear of attack from enemies. Dunn Cavelty has argued that the problem in cyberwar is not the attack itself, but the fear of potential attack.[46] She argues there have been very few attacks that had the potential to rattle an entire nation, or cause a global shock.[47] For example, the loss of revenue, the loss of intellectual property rights and other proprietary data, the costs of maintenance and repair, and increased security costs, together have the potential to reduce public confidence in internet transactions and e-commerce. However, the fear of cyber war is because this attack is new and fear from the actor who conduct the war, which is enemy. Here, there is social construction of what fear is. Fear that the cyber system will not capable to support human's daily life.

Another thing to consider in this constructivist analysis is the construction of identity. Cyber attackers are often identified as enemies in cyberwar. However, when the attack is not from an enemy, but from someone with a similar identity, then it becomes cyber espionage. For example, if Syria cyber attacked the U.S it would count as cyberwar, but if an Australian teenager conducted attack to Microsoft Xbox, it count as espionage because Australia is a U.S ally. Nevertheless, cyberwar is largely driven by state (mis)perception of the interests and identities of other states. If states were to talk to one another, and come to share norms, or respect identity, then perhaps cyber war would be less likely to happen.

Conclusion, which theory is adequate in explaining cyberwar?

For purpose of this essay, I argue that neorealism as a good theory that helps us to understand cyberwar. Liberalism argues that there are many major actors in cyber war. Individuals and the private sector have to be considered as important actors in cyber war. To control behaviour in cyber space, liberals argue that cooperation through institutions is important. However, to date, there are no such strong institutions to control behaviour in cyber space, or to prevent cyber war. Thus, cyber war is still likely to happen. Further, liberals do not explain how norms and institutions can effectively tackle cyber war. Although there are some international institutions, the primary actors are states, not other actors.

Constructivism offers an alternative analysis. National security used to be largely concerned with national sovereignty, but with the development of cyber space, the concept and field of security has been enlarged. In addition, international relations and national security involves perceptions about identities and interests. In order to secure cyber peace, elites need to interact with one another, come to understand different identities and interests, and in this way perhaps come to see the other as a (cyber) friend.

Nevertheless, neorealism is the most adequate theory for understanding cyber war. This theory explains why cyber war happens. Cyber war happens because states, in seeking national security, act 'offensively', in accordance with the 'offence-defence balance' concept. Neorealism provides a more realistic account of the units and processes involved. States are the major actors, and the state of anarchy shapes their behaviour in both the physical and cyber spaces.

References

Adler, E. (1997). Seizing the Middle Ground: Constructivism in World Politics. *European Journal of International Relations, 3*(3), 319-363.

Agius, C. (2013). Social constructivism. In A. Collins (Ed.), *Contemporary Security Studies* (3 ed., pp. 87-103): OUP Oxford.

Barlow, J. (2010). Cyber War and U.S. Policy: Part I, Neo-realism. *The journal of education, community and values, 10*(5), 1-11.

Burchill, S. (2005). Liberalism *Theories of International Relations* (3 ed., pp. 55-83). New York: Palgrave Macmillan.

Caplan, N. (2013). Cyber War: the Challenge to National Security. *Global Security Studies, 4*(1), 93-115.

Cavelty, M. D. (2010). Cyberwar. In G. Kassimeris & J. Buckley (Eds.), *The Ashgate Research Companion to Modern Warfare* (pp. 123-144). Aldershot: Ashgate.

Cavelty, M. D. (2013). Cyber security. In A. Collins (Ed.), *Contemporary Security Studies* (3 ed., pp. 361-378): OUP Oxford.

Choucri, N. (2012). *Cyberpolitics in International Relations*. Massachusetts: MIT Press.

Choucri, N., & Goldsmith, D. (2012). Lost in cyberspace: Harnessing the Internet, international relations, and global security. *Bulletin of the Atomic Scientists, 68*(2), 70-77.

Clarke, R. A., & Knake, R. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*: HarperCollins.

CNN. (2009, 8 July 2009). U.S. government sites among those hit by cyberattack. Retrieved 1 June, 2015, from http://edition.cnn.com/2009/TECH/07/08/government.hacking/index.html?iref=24hou rs

Dunne, T, Kurki, M., & Smith, S. (2013). *International Relations*

Theories. Oxford: OUP Oxford.

Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR) relevant Theory? *International Political Science Review, 27*(3), 221-244.

Gorman, S., Cole, A., & Dreazen, Y. (2009, April 21, 2009). Computer Spies Breach Fighter-Jet Project. Retrieved 1 June 2015, 2015, from http://www.wsj.com/articles/SB124027491029837401

Guilliatt, R. (2015, 2 May 2015). Interpol alerted as teenage hacker from Perth flees to Europe. Retrieved 1 June 2015, 2015, fromhttp://www.theaustralian.com.au/news/nation/interpol-alerted-as-teenage-hacker-from-perth-flees-to-europe/story-e6frg6nf-1227330838160

Hancock, B. (1999). Security views. *Computers & Security, 18*(7), 553-564.

Howard, R. (2014). Richard A. Clarke: Cyberwar in 2013. Retrieved 10 June, 2016, from https://youtu.be/Ewtxa88o6xo

Jervis, R. (1978). Cooperation under the Security Dilemma. *World Politics, 30*(2), 167-214.

Jørgensen, K. E. (2010). *International Relations Theory: A New Introduction*. New York: Palgrave Macmillan.

Kassab, H. S. (2013). In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare. In J. F. Kremer & B. Müller (Eds.), *Cyberspace and International Relations: Theory, Prospects and Challenges* (pp. 59-76). Berlin: Springer.

Katzenstein, P. J. (1996). Introduction: alternative perspectives on national security. In P. J. Katzenstein (Ed.), *the culture of national security: norms, and identity in world politics* (pp. 1-32). New York: Columbia university press.

Kirk, D. (2014, 18 December 2014). North Korea's Cyber Warriors: Privileged Elite In Isolated

Society. Retrieved 9 June 2015, 2015, from http://www.forbes.com/sites/donaldkirk/2014/12/18/north-koreas-cyber-warriors-a-privileged-elite-in-an-isolated-society/2/

Libicki, M. C. (2014). Why Cyber War Will Not and Should Not Have Its Grand Strategist. *Strategic Studies Quarterly, 8*(1), 23-39.

Maximilian,M, Mariana,C & Ruth,.K (2014). The Global Politics of Science and Technology: An Introduction *The Global Politics of Science and Technology - Vol. 1 Concepts from International Relations and Other Disciplines* (pp. 1-38): Springer.

Nazario, J. (2009). Politically motivated of Denial of service attacks. In C. Czosseck & K. Geers (Eds.), *The Virtual Battlefield: Perspectives on Cyber Warfare* (pp. 163-181). virginia: Ios Press.

Rawls, J. (2001). Democratic peace and its stability. In J. Rawls (Ed.), *The Law of Peoples: With, The Idea of Public Reason Revisited* (4 ed., pp. 44-53). USA: Harvard University Press.

Razumovskaya, O. (2015, 8 May 2015). Russia and China Pledge Not to Hack Each Other. Retrieved 1 June, 2015, from http://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/

Rueter, N. C. (2011). *The Cybersecurity Dilemma.* (master of arts), Duke University, Durham.

Shimko, K. L. (2008). Contending perspectives on international politics. In K. L. Shimko (Ed.), *international relations perspectives and controversies* (2 ed., pp. 47-74). Boston: Houghton Mifflin company.Singer, P., & Friedman, A. (2014). *Cyber security and cyberwar what everyone needs to know*. New York: Oxford University press.

Touré, H. I. (2011). *The quest for cyber peace*: international telecommunication union.

Weaver, M. (2009, 8 July 2009). Cyber attackers target South Korea and US. Retrieved 1 June 2015, 2015, from http://www.theguardian.com/world/2009/jul/08/south-korea-cyber-attack