Identifying Cyber Strategies vis-a-vis Cyber Power

Miguel Alberto Gomez
Computer Technology Department
College of Computer Studies
De La Salle University, Manila
Email: alberto.gomez@dlsu.edu.ph
Mobile: +639175382502

***Abstract*—The rhetoric over the rate with which state-sponsored or state-endorsed cyber attacks has grown dramatically in the past years. Increasing dependence on information communication technologies by both state and non-state actors; compounded further by the low-cost of entry and the challenge of attribution within the cyber domain have all but assured that this phenomenon would continue in the foreseeable future. While there is no shortage of literature that discusses the benefits and ease with which these events occur within this domain, their dynamics have yet to be studied through the lens of cyber power. Through the analysis of state cyber power vis-a-vis historical cyber conflicts between states, the study identifies cyber strategies that states may use against each other. The findings provided by this study may go on to aid in establishing appropriate controls to not only mitigate the possible impact of future cyber conflicts but may also lead to the creation of effective deterrence mechanisms.**

I. Introduction

The annual growth of cyber attacks in the last half-decade has triggered concern among global leaders and has driven the need to better understand this phenomenon. Although the prospect of cyber attacks that result in significant damage to a state's infrastructure and massive loss of life still lacks precedence, recent events demonstrate that the growing global dependence on Information Communication Technologies (ICT) increases the likelihood of this occurring. To emphasize this point, in May 2013 the Syrian Electronic Army compromised the Twitter account of the Associated Press (AP) and posted that an explosion that took place in the White House had injured the United States President. This subsequently led to the loss of 136.5B USD on the S&P 500 index. Resulting analysis of the event identified that dependence on automated trading systems that utilized data feeds such as Twitter to execute financial transactions may have contributed to the crash [5]. Although the monetary loss was eventually recovered, this and similar incidents highlight the price required of by the global dependence on ICT.

While controls to mitigate the impact of cyber attacks exist and are driven mainly by the information security industry [23], there are as of yet few studies conducted that addresses the strategy surrounding state-sponsored or state-endorsed attacks[1]. Should the impact of state-sponsored attacks be as great as government leaders perceive them to be, a better understanding of these attacks would be invaluable. Existing studies that attempt to address this have two crucial limitations. The first being their dependence on human expertise to assess the motives and cyber strategies behind the attacks. This is the result of applying International Relations and Political Science theories to explain this phenomenon - the variety of perspectives and schools of thought that exist in this domain inevitably lead to differing expert opinion. The second is a lack of understanding as to how cyber power is manifested in a states cyber strategy. That is to say that while there is an understanding of what factors would make a state capable of launching cyber attacks, the available studies do not bridge the link between capability and action.

To close these gaps, the study proposes that by grouping states based on their perceived cyber power and analyzing the dynamics between these groups, it is possible to identify their cyber strategy that is a result of their respective cyber power.

II. Evaluating Cyber Threats

In light of the decreasing cost of computing equipment and the relative ease with which knowledge may be gained through informal channels, the barriers of entry into cyberspace is significantly lower than that of other instruments of state power such as nuclear weaponry. This enables a larger number of actors to exert varying levels of influence to support their respective interests. Complementary to this is the challenges of attribution that limits certainty in associating a given action with a specific actor. Such anonymity permits actors to operate with little fear of retaliation as the threat of escalation is increased by this uncertainty [16]. With the advantages offered by cyber space as a medium from which atacks may be lanched, the number of state-sponsored or state-endorsed cyber attacks is unlikely to grow in the foreseeable future.

While cyber attacks may be attributed to both state and non-state actors, those that are in-scope of this study are of the former. Consequently, these can be viewed as state-to-state interactions that lend itself for analysis through the lens of International Relations (IR) theories.

[1]As of yet, there is no definite way to distingish the two.

A. Realism

The school of Realism in IR serves as the classical approach to the analysis of security threats[24]. In this particular school of thought, states prioritize their own interests to support their power and security in an anarchic system that threatens these. While the fundamental assumptions of Realism adequately address traditional threats, it falls short when applied to cyber conflict. This is due to Realism's dependence on the state as its primary unit of analysis. The low cost of entry into cyber space, however, allows for non-state actors access to capabilities once reserved for states. Realism fails to take this scenario into account and at best; Realism views cyber conflict as mere extensions of traditional conflict[2] or as economic problems [3].

In a study conducted by Tuthill, Realism may be applied to cyber conflicts if the unit of analysis were to be changed. His study argues that the primary assumptions of Realism applies to cyber space. Central to this claim is the fact that cyber space is itself an anarchic system. Furthermore, it can also be argued that actors in cyber space act independently of each other to further their interests. This is driven by the difficulty of attribution presented by cyber space that results in distrust between actors that eventually lead to unilateral action [25].

While this demonstrates that cyber space takes the form of the environment that Realism assumes to thrive in, the understanding of the nature of states has to be tackled as well. Realism views states in the traditional Westphalian context [24] while in cyber space, there is no clear distinction of states and sovereignty. To overcome this limitation, Tuthill suggests shifting the unit of analysis from the state to security itself. Instead of associating actions with the interest of states, these should instead be viewed relative to the gains or losses in cyber security. While doing so oversimplifies the problem, it allows academics to analyze cyber conflicts free from the restraints imposed by questions of state sovereignty.

From this transformation, applying Realism to the question of cyber conflict gives rise to the following assumptions. First, the global governance of cyber space is not possible. The drive to improve an actor's individual cyber security in this anarchic system takes precedence. This mindset is further justified by the fact that traditional levers of power such as economic, political, military, etc are now being complemented and enhanced by cyber space [23]. From Tuthill's study, unilateral improvement of cyber security benefits these in turn. Consequently, this implies that, to some extent, the proliferation of cyber conflict is to the actor's advantage. Second, while cooperation may still take place, this is simply a means to extend individual interests and does not stem from altruistic ideals. In the case of NATO, while calls for cyber defense have been raised, each individual ally maintains their own strategy [25].

[2]As a means to support existing or future military conflict

B. Liberalism

In contrast with Realism that espouses unilateral action in response to an anarchic system, Liberalism provides insight into the plurality of actors that exists and interacts multilaterally and whose interests go beyond the question of security and survival. Central to the difference between Liberalism and Realism is its acceptance that the idea of state sovereignty is being transformed in lieu of developments in transnational relations as oppose to it losing value [3].

When viewed in the context of cyber conflicts, liberals recognizes the emergence of non-state actors and their influence in this problem domain. More importantly, Liberalism views cyber conflicts as an element of the trans-nationalization of societies and economies. Consequently, this establishes cyber conflicts as not being a spontaneous and short-lived phenomenon but rather as a trend that is most likely to continue in the foreseeable future. From the perspective of academics such as Joseph Nye, the rise of non-state actors in cyber conflicts in terms of their participation and capability is a representation of the power diffusion that is being experienced as a result of the low cost of entry into cyber space [18].

It is, however, important to note that power diffusion does not imply the dissolution of the state as a relevant entity. Rather, it changes the dynamics of state relations. For cyber conflicts, this change is manifested by the addition of a layer of relations that states do not fully control - cyber space and its actors [3]. This is fundamentally different from the value realists assign states and that of Tuthill's revision, as liberals do not insist that the concept of the state has lost its value or has to be reconsidered [18].

C. Constructivism

Whereas realists and liberals depict the extremes in analyzing cyber conflicts, constructivists provide balance and insight as to how this phenomenon emerges rather than attempting to establish that these are fixed realities. Central to this is the belief that social realities are different from material realties and are constantly in flux. Material realities such as computer hardware, security tools, malware[3], etc are believed to be permanent and constant factors. What varies is the manner in which these are applied and the enablers that influence their use.

In his book *People, States, and Fear*, Buzan offers a framework to analyze the vulnerability of states based on their inherent socio-political and military power - whether they are weak or strong in these aspects. While this framework is not quantitative, it does not attempt to identify a fixed reality and illustrates that vulnerability is a function of these

[3]For the purpose of this study, the term malware is used to refer to malicious code that causes damage to systems. Malware that used for information theft is categorized as Information Theft attack.

two attributes. In an effort to apply this framework to cyber conflict, specifically the vulnerability of states to cyber attack, Hare modified the said matrix in his respective paper [13].

To further evaluate the perspective offered by constructivists, the Cyber Power Index developed by Booze Allen Hamilton gives insight as to how states with presumably the same interests and capabilities can still differ in terms of their cyber power [12]. For the analysis performed by Booze Allen Hamilton, the G20 states were used[4]. If the perspective of the realists is to be utilized, then these states that are economically similar and exist in the same anarchic system should have the same interests and their actions may be explained uniformly. For liberals, the interconnectedness of these economies means that they all face relatively the same level of vulnerability that stems for this interconnectedness. However, when the result of the index is compared with cases of cyber conflicts faced by these states, realism and liberalism fail to provide uniform explanation of these events. For example, in the case of the United States and Australia, while both rank within the Top 3 of the index, the number cyber attacks faced by the United Sates id disproportionate to that of Australia despite their average ranks which is a product of legal and regulatory frameworks, economic and social context, technology infrastructure, and industry application attributes. From a constructivist's perspective, the difference may be explained by variations in the attributes that determine a state's cyber power and, consequently, the realities it faces.

III. Methodology

A. Measuring Cyber Power

While reliance on theory may be adeqaute for academic study, policy makers and security professionals require empirical evidence in order to deploy adequate security controls and deterrence mechanisms.This requires knowledge of individual state cyber capabilities vis-a-vis their predisposition to use such as a means to achieve their objectives.

Borrowing Nye's definition, cyber power may be defined as *the ability to obtain preferred outcomes through the use of the electronically interconnected information resource of the cyber domain* [13]. Given this, it should be emphasized that cyber power exists as an end state - the product of a state's ability to convert resources that it possesses into enablers that allow it to obtain the outcomes it desires. While it can be argued that these power enablers are similar across states, what differentiate them are their abilities and/or willingness to convert these resources into cyber power.

The Cyber Power Index (CPI) was developed by Booze Allen Hamilton as a means to measure state cyber power that they define as *the ability to withstand cyber attacks and to deploy the digital infrastructure necessary for a productive and secure economy.* To this end, they propose four general components that contribute to a state's cyber power. These are existing legal and regulatory frameworks[5], economic and social context[6], technology infrastructure, and industry application [12]. In effect, the CPI attempts to explicitly measure a state's ability to survive cyber attacks and implicitly, its offensive capabilities.

While it may be tempting to simply attribute cyber power to offensive capabilities as is indirectly provided for by the CPI, a state's willingness to invest its resources to achieve a specific goal is inversely proportional to its inherent vulnerability that may be exploited by retaliatory action. Simplified, a state will not willingly exercise its cyber power to the fullest if it is aware of significant damage that may result from retaliation [16]. In identifying vulnerability, Buzan and, consequently Hare, propose that a state's military power and socio-political cohesion contribute to this by mapping these factors against the perceived vulnerability of a state. One key difference between Hare and the CPI though is his use of the categorical terms High and Low to define these attributes as opposed to the CPI's use of quantitative attributes.

Taking into consideration the interdependence of both offensive capability and inherent vulnerability, this study utilizes an amalgamation of features from both the CPI and Hare in order to describe a state's perceived cyber power. The study identifies 50 individual features that may be consolidated into 6 feature groups: Infrastructure [2] [1], Economic [2] [9], Research [2], Policy & E-Governance [2] [1] [14] [19], Socio-Political Cohesion [2] [20] [15] [8], and Military Strength [22]. While it would be ideal to obtain the most recent values for the respective features, this was not always possible as the collection period used by the sources are not uniform. As a rule, the study limits itself to features that are not missing in more than 50% of the states that are being studied. In cases where this parameter is not met, the average of the dataset for that missing feature is used.

B. Identifying Cyber Power Groups

While cyber power varies between certain states, they can still be grouped based on their relative similarities. In this case, states are clustered[7] based on the relative similarity of the identified features.

As mentioned in earlier sections, relationships between states may be explained through the use of different IR theories. In relation to this, the theories may also be applied to group similar states together with respect to their behavior. Such an approach, however, is limited by (1) the interpretation of the respective theories and (2) focus on the end result of

[4]Focus solely on these states tends to limit the usefulness of the Cyber Power Index

[5]Legilstaion against cyber crime, adherence to international treaties, etc.

[6]The use of ICT by to the knowledge economy and society.

[7]An exploratory data mining technique

state interaction rather than the enabling factors. Though IR theories lend themselves well to the problem domain at hand, the variety of theories available to explain and group states are numerous and are not necessarily compatible with each other. Consequently, this leads to conflicting perspectives that cannot yield a unified view of the problem domain. In relation to this, most of the theories discussed in previous sections answer the question of "why" states behave instead of "how" or what the enabling factors are surrounding these.

C. Linking Cyber Power to Cyber Conflict

Although grouping states by means of their cyber power provides insight that has yet to be explored, respective cyber strategies can only be identified if cyber capabilities are analyzed in the context of past cyber attacks. To understand the relation between cyber strategy and cyber power, cyber strategy is defined as *the development and employment of strategic capabilities to operate in cyber space, integrated and operated with other operational domains, to achieve or support the achievement of objectives across the elements of national power in support of national security strategy* [11]. As capability eventually translates to cyber power, a state's cyber strategy is a reflection of its cyber power.

For this study, information concerning past cyber attacks are analyzed in terms of the following parameters: initiator, target, attack type, attack severity, and frequency[8]. It should be noted that cyber attacks, as defined by this study, does not consider every individual case of a computer system being compromised. Rather, it views these instances as part of a larger operation. Data regarding cyber attacks are gathered from the study conducted by Valeriano and Maness [26] and through Hackmageddon.com [21] - an open initiative that tracks global cyber attacks.

IV. Results and Analysis

A. Cyber Power Groupings

Once the respective cyber power features are analyzed, four distinct state groups[9] emerged based on their respective cyber power as seen in Table I. Statistical analysis techniques

TABLE I
GROUP MEMBERSHIP

State Group	Members
Established Passive I (EP-I)	US
Emerging Aggressive II (EA-I)	CN
Established Passive II (EP-II)	AU, CA, NZ, SG, JP, KR, PH, RU, IL
Emerging Aggressive II (EA-II)	CL, ID, MY, MX, PE, TH, VN, IN IR, PK, BD, SY, CY, TR, IQ, KW, GE, LB

are used to provide insight into each cluster, feature group, and cyber attacks (see Table II). By comparing these three, the respective cyber strategy per group, and in effect per member state, can be identified. The recently published *World War C* report from FireEye that identifies specific strategies from captured cyber activities further supports the results in this section [6].

States that have been identified as Established Passive I and II are seen as having the most matured and developed Infrastructure, Economic, Research, and Policy & E-Governance mechanisms in place. EP-I and EP-II differ mainly with regards to their respective Socio-Political Cohesion and Military Strength features where EP-II is higher in the former and EP-I is higher with respect to the later. The existence of high values for the first four feature groups is unsurprising as these are all positively correlated with each other which indicates that as each of these increases, the others increase in turn.

States that were identified as being members of EA-I and EA-II display lower Infrastructure, Economic, Research, and Policy & E-Governance with respect to the other two groups but have noticeably higher Socio-Political Cohesion and the highest Military Strength with respect to EA-I. Quantitatively, the data indicates a negative correlation between the first four feature groups and Socio-Political Cohesion. It should also be noted that members of the these two groups may also be considered as part of emerging economies whose Infrastructure and Economic capability are still being developed. With regards to the Military Strength of EA-I, this is unsurprising as China is considered to be the Top 3 in terms of Military Strength according to Global Firepower [7].

B. Identified Cyber Strategies

The identified cyber strategies in the following subsections were obtained by analyzing the identified groups vis-a-vis the observed cyber attacks. These cyber attacks are analyzed based on their frquency and directionality (source and destination).

1) Established Passive I, Maintaining Power: The analysis of the cyber attacks experienced and launched by the United States, the sole member of the Established Passive I group, paints a picture of an entity that aims to prevent the rise of states that may challenge its position. In terms of the directionality of cyber attacks being launched by EP-I, the target of these cyber attacks are solely EA-I and EA-II. Specifically, EP-I utilizes malware as the primary mode of attack against its targets. When analyzed against the different feature groups, the use of malware as a primary tool for cyber attack is positively correlated with the initiator's Military Strength. From a realist's perspective, this can be explained as a form of containment. In the case of the Stuxnet attacks against Iran by the US, the presumed use of malware to disrupt uranium enrichment by damaging the devices used for these operations is a clear example of attempts to curtail Iran's attempts to develop greater nuclear capability - a threat perceived by the US [4]. The use of malware minimizes the risk of escalation even if the source of the attack is identified

[8]Based on the study conducted by Valeriano and Maness[26]
[9]Term used in place of clusters

TABLE II
ATTACK TYPE MATRIX

	Target			
Initiator	**EP-I**	**EA-I**	**EP-II**	**EA-II**
EP-I	NA	Malware	NA	Malware
EA-I	Information Theft	NA	Malware	Malware
EP-II	Malware	Defacement	DoS/DDoS	Malware
EA-II	Defacement	NA	DoS/DDoS	Defacement

as there remains a degree of ambiguity as to its author [10]. This is supported in the *World War C* Report that identifies the objectives of the United States as being information gathering and subtle system disruption [6]

What is noticeable from the data is the lack of attacks being initiated by EP-I against EP-II states. There are two explanations for this lack of cyber activity. One is the fact that most members of EP-II are allies of EP-I and as such are not viewed as threats. In relation to this, the United States also maintains strong political and economic ties with members of EP-II and as such share common interests and benefits that may be disrupted in the event of perceived aggression by EP-I.

2) Emerging Aggressive I, Maneuvering Into Position: As previously mentioned, states that are grouped as Emerging Aggressive are considered emergent in terms of Infrastructure, Economy, Research, and Policy & E-Governance. Amongst these, EA-I and its sole member the People's Republic of China (PRC) stand to match the levels of EP-I and EP-II states. While politicians and the media have been actively portraying the PRC as a revisionist power in light of recent activities in both the real world and cyber space [11], the information garnered from this study illustrates a more complex scenario in which aggressive action in cyber space is calculated to minimize risk to the initiator and to allow for a certain degree of deniability.

In terms of cyber attacks launched by EA-I, the primary targets are EP-I and EP-II states with a few being directed towards EA-II - most notably the Republic of the Philippines. This trend of attacking states that show greater development in terms of the first four feature groups is expected from a state this is maximizing the power it currently has to gain advantages possessed by others [24]. Data from the *World War C* report supports this as it identifies the PRC's primary motive as being economic espionage and persistent access [6]. This is best seen in information theft attacks launched against the United States. Based on the data obtained from this study, the number of information theft attacks launched increases relative to the Military Strength of the initiator. That is to say that, as with malware, the greater the Military Strength of the initiator, the more likely it will opt for this strategy. Supporting this is the fact that states with high levels of the first three features has the greatest chances of experiencing these attacks. The primary reason behind this trend is that these features are all crucial for growth and development. As such, emergent states would desire acquiring information that may give them advantages in this regard. The question though, is why does the PRC use a different strategy when it comes to EP-II states - opting for malware over information theft.

While the parameters for initiating malware and information theft attacks are similar, the risk of escalation from each differs. This difference is a function of the visibility of each attack. Most cases of information theft are learned of after the fact; usually these operations have existed for years before coming to light [17]. Malware threats aimed at disrupting specific systems, manifest their presence faster. From the perspective of Socio-Political Cohesion, the number of information theft and malware attacks should be lower for states that have higher Socio-Political Cohesion - as is the case for EP-II. This is due mainly to the fact that the citizenry may clamor for a strong state response to these attacks - especially visible and damaging attacks [16]. This, however, may be tempered if the initiator's Military Strength is compared to the target's. A large imbalance between the initiator's Military Strength and the target's may discourage a strong response despite calls for such. But should this difference be narrower and the presence of additional complications[10], the initiator may favor a more subtle attack. This argument may be presented as a means to justify the difference between attacks launched against EP-I and EP-II states.

3) Established Passive II, Maintaining the Status Quo: While the previously discussed groups demonstrated a penchant for actively stoping the growth of rivals or to actively engaging in actions to obtain necessary advantages, states that belong to EP-II tend to demonstrate a balanced and distributed strategy across the different state groups and even towards its own members. Most notable amongst the actions of this group are malware attacks directed towards EP-I and EA-II states. As mentioned in the previous section, malware attacks are used sparingly as these can quite easily lead to an escalation of conflict. In the case of malware attacks launched by the Russian Federation against the United States, the narrow difference between the military capabilities of these two removes any hesitation of launching such attacks. This confidence in choosing this course of action may also be attributed to low Socio-Political Cohesion for both

[10]Such as the proximity of the target's allies to the initiator.

EP-I and EP-II and coupled with the existence of relatively liberal governments which further subdues the likelihood of escalation. The same explanation may also be extended to cases of cyber attacks between EP-II and EA-II. With both having comparable Military Strength, no clear advantage can be gained through escalation into an actual physical conflict.

EP-II cyber attacks towards EA-I, initiated primarily by the Republic of the Philippines, provides a counterpoint to the explanation of cyber strategies that have been encountered up to this point. Whereas previous strategies have been used to minimize calls for retaliation while maximizing gain, defacement attacks launched against the PRC function as a means to show a response while still minimizing the likelihood of kinetic retaliation. Amongst all the attack types, defacement is the least damaging and easiest to launch and attribute. From a strategic standpoint, this offers the initiator three advantages. First, it demonstrates a response to its citizenry thus minimizing further calls for action [16]. Second, it does not require a high degree of technical skill; consequently allowing a larger number of states to utilize this. Lastly, since this is easier to attribute and causes minimal damage, targets may not necessarily be driven to execute a strong response thus reducing the chances of escalation.

In terms of attacks launched against its own members, the use of DoS/DDoS also follows the same line of reasoning as defacement attacks and takes advantage of the fact that these attacks are highly visible and easier to attribute than information theft and malware. While some would argue that DoS/DDoS attacks are highly damaging to states with a high dependence on their infrastructure, the maturity of the said infrastructure also allows for resilience against such attacks - in turn, minimizing impact. It should be pointed out, however, that members of this group still engage in information theft primarily as a means of gaining tactical and strategic advantges [6], though not in the same extent as EP-1 and EA-II.

4) Emerging Aggressive II, Testing the Waters: Of all the states in scope of this study, those grouped as EA-II are considered to be the weakest in terms of cyber power. The use of either defacement or DoS/DDoS attacks by these states illustrate that their primary strategy is to demonstrate capacity while minimizing the risk of coming into conflict with states that are better established. As these states demonstrate the highest levels of Socio-Political Cohesion amongst the other groups identified in this study, their respective populace may possesses stronger nationalistic fervor that may explain their use of these types of attacks. However, the use of such attacks does not provide them with advantages to increase their capabilities - in contrast to EA-I. Consequently, these states are still dependent on enhancing their respective cyber power through less aggressive means. As such, they cannot be said to be practicing a consistent cyber strategy.

V. Conclusion

Based on the results, there are at least three primary cyber strategies that states can utilize in order to take advantage of their respective cyber power and the inherent nature of cyber space: *power maintenance*, *balance maximization*, and *capacity demonstration*.

The *power maintenance* cyber strategy entails that states will actively utilize cyber space as a means to mitigate perceived threats to their power. Such action would include using malware to disrupt capabilities of rival states and as a means to demonstrate the initiator's capabilities. Such a strategy, however, can only be utilized if the initiator is confident of its ability to contain or address any possible escalation that may result from these cyber attacks. As such, Military Strength is of crucial consideration for this strategy. Moreover, the reason behind this strategy can also be explained through realist theory as it is a direct manifestation of a states willingness to protect its interests.

The *balance-maximization* cyber strategy, on the other hand, entails that states will attempt to maximize the power they currently have in order to gain advantages in both cyber space and the real world but not at the cost of triggering further conflict that may endanger the advantages (such as economic) that they currently posses. As such, information theft and malware attacks are most likely to be launched by states that practice this strategy. While this follows realist ideas similar to that of power maintenance, it also takes into consideration the implications of being interconnected and the negative consequences this may have on the initiator if this strategy is not utilized judiciously.

Lastly, the *capability demonstration* cyber strategy is used primarily by states as a means to demonstrate emergent capabilities in cyber space. As such, this is the least effective of all the existing strategies. The imperative for states to utilize such a strategy exists when the situation demands a response without the risk of escalating the existing conflict further. It should be noted, however, that this strategy is not limited solely to EA-II states. More advanced states may opt to use this strategy if the previous strategies are excessive or may lead to even greater conflict. Capability demonstrations can also serve as a means to deescalate an existing conflict by giving the populace the appearance that a state has responded while less forceful measures, such as negotiations, can take place in the background. Defacement and DoS/DDoS attacks may be used by states to this end.

While the study offers insight as to how states may utilize their respective cyber power, further work is needed in order to understand this phenomenon. Questions such as private-public sector involvement in executing these strategies, deterrence strategies, and the legalities of actions in cyber space are all important issues that must be addressed before

it can be claimed that the phenomenon of cyber conflict is well understood. To this effect, the study provides the crucial first step from which these other studies may be initiated.

REFERENCES

[1] Itu ict eye. [Online]. Available: http://www.itu.int

[2] World bank data. [Online]. Available: http://data.worldbank.org

[3] *The Information Revolution, Security, and International Relations IRrelevant Theory?*, vol. 27, 2006.

[4] P. Beaumont and N. Hopkins. (June) Us was key player in cyber-attacks on iran's nuclear programme. [Online]. Available: http://www.guardian.co.uk/world/2012/jun/01/obama-sped-up-cyberattack-ira

[5] W. K. Eric Lam, Lu Wang. Fake post erasing $136 billion shows market sneed humans. [Online]. Available: http: //www.bloomberg.com/news/2013 - 04 - 23/fake - report - erasing - 136 - billion - shows - market - s - fragility.html$

[6] FireEye, "World war c: Understanding nation-state motives behind todays advanced cyber attacks," FireEye, Tech. Rep.

[7] G. Firepower. Global firepower. [Online]. Available: http://www.globalfirepower.com

[8] I. for Democracy and E. Assistance. Voter turnout. [Online]. Available: http://www.idea.int

[9] K. for Development. Kei and ki indexes. [Online]. Available: http://info.worldbank.org

[10] A. M. Freed. Red october malware attacks highlight attribution problems. [Online]. Available: http://www.bloomberg.com/news/2013-04-23/fake-report-erasing-136-billion-shows-market-s-fragility.html

[11] M. A. Gomez, "Awaken the cyber dragon: China's cyber strategy and its impact on asean," *Journal of Communication and Computer*, 2013.

[12] B. A. Hamilton, "Cyber power index: Findings and methodology," Booz Allen Hamilton, Tech. Rep.

[13] F. Hare, "The cyber threat to national security: Why we can't agree," in *Conference on Cyber Conflict Proceedings 2010*, 2010, pp. 211–225.

[14] O. Initiative. Opennet initiative. [Online]. Available: https://opennet.net

[15] T. International. Corrpution perception index. [Online]. Available: http://cpi.transparency.org

[16] M. C. Libicki, "Sub rosa cyber war," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, C. Czosseck and K. Geers, Eds. IOS Press BV, 2009.

[17] Mandiant, "Apt1: Exposing one of china's cyber espionage units," Mandiant, Tech. Rep.

[18] J. S. Nye, *The Future of Power*. PublicAffairs Books, 2011.

[19] U. N. D. of Economic and S. Affairs. United nations e-government survey 2012: E-government for the people. [Online]. Available: http://www.un.org

[20] W. H. Organization. Suicide rates per 100,000 by country, year and sex. [Online]. Available: http://www.who.int

[21] P. Passeri. Hackmageddon.com. [Online]. Available: http://www.hackmageddon.com

[22] J. D. Singer. Correlates of war. [Online]. Available: http://correlatesofwar.org

[23] S. H. Starr, "Towards a preliminary theory of cyberpower," in *Cyberpower and National Security*, S. H. S. Franklin D. Kramer and L. K. Wentz, Eds. Potomac Books, Inc, 2009.

[24] P. Sutch and J. Elias, *International Relations: The Basics*. Routledge, 2007.

[25] D. P. Tuthill, "Reimagining waltz in a digital world: Neorealism in the analysis of cyber security threats and policy," Ph.D. dissertation, University of Kent, March 2012.

[26] B. Valeriano and R. Maness. Cyberwar and rivalry: The dynamics of cyber conflict between antagonists, 2001-2011. [Online]. Available: http://wpsa.research.pdx.edu/meet/2012/manessvaleriano.pdf