STRATEGIC ASSESSMENT OF ISIS CYBER COMMAND

By

Dr William P. PETER
School of Management
University of California
Oakland, California
United States

ABSTRACT

This study examined the strategic assessment of ISIS Cyber Command. Two specific research objectives were formulated to guide the study. The research design was descriptive survey design research design. The population of the study comprised of all professionals in computer science, computer engineering and security agents who have been exposed to computer science using a stratified sampling technique. The instrument known as "ISIS Cyber Command Questionnaire" (ICCQ) was used to collect the data. The instrument was subjected to reliability test, using test-retest method and it produced high average reliability coefficient of 0.82 to justify the use of the instrument. The analysis was done using appropriate statistical techniques such as regression analysis. The findings revealed that there are many cases of operations of ISIS Cyber Command, cyber conflicts in the globe. There is significant implication of the operations of ISIS Cyber Command on cyber conflicts in the globe. Finally, the operations of ISIS Cyber Command have negative effects on the global economy. One of the recommendations was that international training courses on countering violent extremism (CVE) should be developed.

Key Words: Cyber conflicts, Cyber command, global economy

INTRODUCTION

In recent months the Islamic State, formerly known as the Islamic State of Iraq and al-Sham (ISIS) has managed to position itself as the most significant threat to regional stability in the Middle East. The Islamic State is a linear descendant of Abu Mus'ab al-Zarqawi's "the Organization of Jihad's Base in the Country of the Two Rivers", which was commonly known as Al Qaeda in Iraq (AQI) formed in 2004 to fight the American invasion of Iraq (Hoffman, 2006). In the last year, IS strategic military campaign has taken over large swaths of Syria and Iraq at lightning speeds, taking its opponents by surprise. Its political and ideological campaign is equally aggressive; it has taken on the Internet and social media by storm. IS has forced a sea of change in the way we understand modern terrorism. IS has not eclipsed Al Qaeda, which is still very relevant and dangerous, but it has physically broken away from Al Qaeda's leadership. IS continues to profit from the roots of Al Qaeda's already highly developed communications strategy.

According to Philip (2016), ISIS builds upon a decade of experience, in its ability to intimidate, radicalize, recruit, train and extort. IS is different from other terrorist organizations of the past for a multitude of reasons: first, its construction of a pseudo state, an "Islamic Caliphate"; second, its ability to sustain itself economically by amassing greater riches than any terrorist organization in the past; third, its globalist and apocalyptic ambitions and its heady millenarianism; and finally, its powerful social media campaign, that has a global following, which has to date attracted over 18,000 foreign fighters from over 90 countries (Zelikow, 2003).

According to Desmond (2002), ISIS's main effort to date in cyberspace has focused on psychological warfare by generating fear through flooding the internet with video clips portraying the brutal acts of beheading and mass executions, as well as victory parades, as part of developing deterrence and creating an illusion of force in excess of the organization's actual strength. The essence of its online activity, however, is broader. It enables its supporters to obtain operational information, including training in preparing explosives and car bombs, and religious rulings legitimizing massacres in regions under ISIS control. The attack launched by ISIS has remarkably affected the global economy and the peace of other nations eventually leading to the cyber conflict among nations. This study therefore strategically assesses ISIS cyber command in the above directions.

Statement of the Problem

Recent events in Iraq are liable to give new impetus to the ideas and the path that ISIS represents, which are shared by many terrorist organizations operating in the Middle East and beyond. Its strong economic capacity could be exploited to support and acquire influence over the operations of terrorist organizations that share its ideas. In addition, enormous quantities of high quality weapons, many of them Western, have fallen into ISIS hands, and they will certainly find their way to terrorist organizations operating in combat zones in the Middle East and even beyond. Like many other countries in the world, Israel is watching the development of the battle in Iraq with great interest. While it appears that at this stage there is no immediate threat to Israel's security from the events in Iraq, the resulting atmosphere could strengthen global jihad elements operating in countries near Israel. The IS crisis has become one of the most documented and socially-mediated conflicts in history, creating much effect on the global economy and leading to the cyber conflict among nations. It is on this premise that this study is conducted for the purpose of strategic assessment of ISIS cyber command with respect to its effect on global economy and cyber conflict among nations.

Objectives of the study

The main objective of this study is to carry out the strategic assessment of ISIS Cyber Command with respect to its implications on cyber conflicts and global economy. Specifically, the following objectives have been drawn:

1. To find out the implication of the operations of ISIS Cyber Command on cyber conflicts in the globe.
2. To examine the implication of the operations of ISIS Cyber Command on the global economy.

Hypotheses

The following hypotheses will be tested:

1. There is no significant implication of the operations of ISIS Cyber Command on cyber conflicts in the globe.
2. There is no significant implication of the operations of ISIS Cyber Command on the global economy.

Significance of the Study

This study is of great importance to the armory of military forces and security services in their battle to fight terrorism in the nation. It will expose them to various ISIS cyber commands

and capabilities and hence bring awareness on the terror group. The result of this study will be beneficial to the public, in that they will be aware of cyber terrorism and know how to avoid it.

This study will be of value to the policy makers and regulators such that they will gain insight on ISIS cyber command strategy. This will influence policy makers formulating informed policies concerning the overall security of the country. This study will also provide basis for future researchers on relevant topics. The scholars, computer science students and ICT professionals, security agents will find this study valuable as they will gain knowledge to carry out further security studies on the topic.

LITERATURE REVIEW

CONCEPT OF ISIS CYBER COMMAND

The brutal actions of IS in Syria and Iraq are nothing new for those following its evil deeds since it announced its establishment some eighteen months ago. However, for the last two months the organization's name has been mentioned repeatedly by world leaders as a significant threat, particularly since in recent months ISIS has conquered large swathes of Iraq and also threatened to attack and capture Baghdad, on its way to taking control of all of Iraq. These moves were accompanied by killing sprees that were extraordinary in their scope and cruelty, and that in recent weeks reached new depths with the mass slaughter of the defenseless Yazidi minority (Conway, 2003). Without minimizing the achievements of IS, it appears that the secret of its power rests primarily on the weakness of its enemies. So far, IS has made territorial gains only in Iraq and in limited areas of Syria, two failed states whose central governments suffer from a lack of legitimacy among their citizens and ineffective control of large parts of their territory. The Iraqi army has proven a spiritless failure, while in Syria the army is mainly engaged in maintaining the survival of the regime in the country's principal cities (US Department of Defense, 2012).

Hoffman (2006) asserts that the main danger posed by IS does not concern the integrity of countries in the region, but its ability both to channel money and advanced weapons to terror organizations active in the region, and to make the territory it controls, which connects western Iraq with northern and eastern Syria, an impervious haven. This could serve as a base for promoting subversive activity and spreading terror, which in turn would increase regional instability.

Cyber jihad plays a key role in ISIS strategy, and hence the urgent need to contend with the challenge that it poses to the international coalition fighting the terrorist organization. The use of cyberspace by ISIS has helped the organization brand itself in the global discourse as an entity that evokes terror, deters its enemies, and lures new supporters and operatives to its ranks. The centrality of cyber jihad as a tool for recruitment, radicalization, and dissemination of propaganda makes the struggle against ISIS's use of cyberspace no less important than the physical engagement with its forces and the prevention of its geographic expansion. Both the use of cyber-terrorism through the Internet and social media have been by extremist groups in order to manufacture a process of online hate. In the case of many of the tweets and videos analyzed in these cases, the Internet and social media sites act as a knowledgeable database on how to promote violence as a strategy through the social learning theory (Freiburger and Crane, 2008). This theory asserts that individuals learn deviant behaviour from other groups, which may lead to extremist learning that is categorized by association, definitions, differential reinforcement, and

imitation. They argue that mechanisms of the social learning theory are used by terrorist groups on the Internet as a tool to facilitate attacks and recruitment (Desmond, 2002). It also shows how social media sites online have been used by ISIS to create a terror network.

Freiburger and Crane (2008) refer to a European case study where Peter Cherif was recruited by Al-Qaeda over the Internet through a similar learning process (Powell, 2005). They argue that if groups become marginalized they become more susceptible to using the Internet for terrorist purposes. The use of social constructionism as a mechanism to understand the competing definitions of cyber-terrorism is crucial in getting a better understanding of the phenomena. Clearly, social practices and social behaviour change with time and thus our understanding of online extremism will also evolve. Within this context social constructionism offers both criminologists and sociologists a means to examine the various social processes that emerge when looking at interpretations of online extremism (Felson, 2002). ISIS is not explicitly attempting to recruit sophisticated hackers, but its followers can broaden their knowledge and skills through hacking courses, tools, and guidance available in Deep & Dark Web forums. Pro-ISIS cyber actors are likely to download hacking tools from publicly available sources while also utilizing both off-the-shelf and custom malware.

GLOBAL ECONOMY

Global economy as the economy of the world, considered as the international exchange of goods, has been much affected by cyber crime and other militating forces, (World Economic Situation and Prospects, 2018). Beyond the minimum standard concerning value in production, use and exchange, the definitions, representations, models and valuations of the world economy vary widely. Most times questions of world economy is limited exclusively to human economic activity and the world economy is typically judged in monetary terms.

In a situation where there is market with clarity and efficiency to establish a monetary value, economists do not typically use the current or official exchange rate to translate the monetary units of this market into a single unit for the world economy since exchange rates typically do not closely reflect worldwide value. According to World Bank, (2011) market valuations in a local currency are typically translated to a single monetary unit using the idea of purchasing power. However, the world economy can be evaluated and expressed in many more ways. It is unclear, for example, how many of the world's 7.13 billion people have most of their economic activity reflected in these valuations.

The global economy is the sum total of the economies of individuals, corporations and all nations in existence today. It is influencing the economies of individual nations and at the same time being influenced by macroeconomic policies of the individual nations and the economic policies of world bodies like the World Trade Organization, World Bank, International Monetary Fund, etc. Protectionism, a significant component of the 16th mercantilist economist system that emerged in Europe, is still being pursued to protect national economies from the perceived and real threats of globalism and international competition. It has repercussions for the global economy. The global economy too, as product of the forces of globalization, has acquired certain features and components which define its anatomy and strengthens its influence on or reactions

to protectionist policies. The goals of this article are examining the anatomy of the global economy in the era of globalization and explaining its implications for protectionism.

ISIS CYBER COMMAND AND GLOBAL ECONOMY

According to the World Economic Forum (2015), security experts believe that hacking attacks in support of the operations conducted by members of the Islamic sect are a concrete threat to the economy. In spite of the numerous cyber-attacks conducted by cells and sympathizers of the radical organizations, the overall capabilities are not advanced. The experts speculate that in the short term the members of the Islamic State will not be able to increase the level of sophistication of the attacks. In the last couple of years, the ISIS has increased its hacking activity in a significant way, at least five different pro-ISIS hacking group launched cyber-attacks in favor of the Islamic State. In many cases, the same hackers supported the different groups in multiple attacks. It has become obvious that these attacks have not only affected the economies of the victim countries but has also had an extension to the global economy.

According to Graham, (2017), in 2016 "cybercrime cost the global economy over $450 billion, over 2 billion personal records were stolen and in the U.S. alone over 100 million Americans had their medical records stolen," said Steve Langan, chief executive at Hiscox Insurance, told CNBC. "This is an epidemic of cybercrime, and yet 53 percent of businesses in the U.S., U.K. and Germany were just ill-prepared."U.S. firms are most prepared in case of an attack, with 49 percent of expert-ranked companies coming from the states. Of note, larger U.S. firms were the most targeted with 72 percent being attacked in the past 12 months.

According to the Anti-Terrorism Coalition (ATC), the jihad was organized by a group named Osama Bin Laden (OBL) Crew, also threatening attacks against the ATC website (ATC, 2004). According to Internet Haganah (2006), cyber attacks have created many damages to the economy of every nation that encounter such attack. Wakeford (2015) reported one example of custom malware used by members of a pro-ISIS group in late 2014 that was masquerading as a slideshow and spread via Twitter. The analysis of the binaries detected by the experts revealed that it is a very simple sample of customized malware. He asserts that e*ven though it was not complex or sophisticated, it was enough to identify and geolocate the infected machines and their owners. In other words, pro-ISIS cyber threat actors have a record of distributing malware via social media, affecting thousands of computer systems in a minute and causing much loss to the affected organizations and countries*.

Jenkins (2003) asserts that "the advancement of the cyber capabilities of pro-ISIS actors largely depends on the group's ability to bring in a technological savvy, diverse group of people with broad technical skills. Hussain, who joined ISIS as a somewhat sophisticated hacker, given his time with TeaMp0isoN, is a good example and set the precedent". Organizations that comprise the critical infrastructure of the national economy should be aware of the potential for terrorist attack (Nickolov, 2005). Critical infrastructure refers to the essential assets which make society or a country function well and includes energy, transportation, telecommunication, water supply and waste management, agriculture and food supply, finance, public health, and essential

government services. Organizations which form the critical infrastructure of a national economy must protect their information systems well.

METHODS

Research Design

The researcher adopted a descriptive survey design. This type of design creates a platform for the researcher to make full description of the causes, effects and extent of the effects caused by the variables.

Area of the Study

The area for this study was Nigeria as the giant of Africa.

Population of the Study

The population of this study consisted of all professionals in computer science, computer engineering and security agents who have been exposed to computer science.

Sample and Sampling Techniques

The researcher used a stratified random sampling technique in selecting to draw the 300 respondents for the study.

Instrumentation

The main instrument used in this study was questionnaire titled "ISIS Cyber Command Questionnaire" (ICCQ). The questionnaire comprised sections A and B. Section A contained information on personal data of the respondents while section B contained three variables such as operations of ISIS Cyber Command, cyber conflicts, and global economy. The obtained data were coded for the statistical analysis.

Validation of the Instrument

The instrument used for the research was made to pass through face and content validation using experts in computer science.

Reliability of the Instrument:

The researcher used Cronbach Alpha reliability technique to measure the level of reliability of the instrument, using 40 respondents who were not part of the main study. The test helped to produce reliability coefficient of (0.82) which passed reliability and justification of the instrument.

Procedure for Collecting Data

The researcher used a letter of introduction to gain the respondents audience. This letter helped introduce the researcher to the respondents for acceptance and assistance. The questionnaire issuance and retrieval took about eight days.

Method of Data Analysis

The researcher subjected the data generated to appropriate statistical techniques such as regression analysis. The test for significance was done at 0.05 alpha levels.

RESULTS AND DISCUSSIONS OF THE FINDINGS

Results

Hypothesis One

There is no significant implication of the operations of ISIS Cyber Command on cyber conflicts in the globe.

Table 1

Regression analysis on the implication of the operations of ISIS Cyber Command on cyber conflicts in the globe.

Variable	R	R Square	Adjusted R Square	Std. Error of the Estimate
Operations of ISIS Cyber Command	0.92*	0.85	0.85	0.57

***Significant at 0.05 level; df =298; N =300; critical r–value = 0.113**

Table 1 reveals the weight of the relationship between the independent variable (Operations of ISIS Cyber Command) and the dependent variable (Cyber Conflict). The value of R, depicting the correlation coefficient of 0.92, is the linear correlation between the observed and model-predicted value of the dependent variable (Cyber Conflict). Its big value (0.92) indicates a strong positive relationship between the variables. R^2; the coefficient of determination, (0.85) is the squared value of the correlation coefficient. It shows that 85% of the variable (Cyber Conflicts) is explained by the model (Operations of ISIS Cyber Command). The result means there is corresponding linear implication of the operations of ISIS Cyber Command on cyber conflicts in the globe.

Hypothesis Two

There is no significant implication of the operations of ISIS Cyber Command on the global economy.

Table 2
Regression analysis of the implication of the implication of the operations of ISIS Cyber Command on global economy.

Variable	R	R Square	Adjusted R Square	Std. Error of the Estimate
Operation of ISIS Cyber Command	0.94*	0.88	0.88	0.47

***Significant at 0.05 level; df =298; N =300; critical r–value = 0.113**

Table 2 reveals the strength of the relationship between the independent variable (Operations of ISIS Cyber Command) and the dependent variable (Global Economy). The value of R depicting the correlation coefficient of 0.90, is the linear correlation between the observed and model-predicted value of the dependent variable (Global Economy). Its big value (0.94) indicates a strong positive relationship between the stated variables. R^2, the coefficient of determination, (0.88) is the squared value of the correlation coefficient. It shows that 88% of the variable (Global Economy) is explained by the model (Operation of ISIS Cyber Command). The result means that there is corresponding linear implication of the operations of ISIS Cyber Command on the global economy.

Discussion of the findings

The result of the data analysis in Table 1 was significant due to the fact that the calculated R-value (0.92) was greater than the critical R-value (0.113) at 0.05 level, with 298 degree of freedom. The result implies that there is significant implication of the operations of ISIS Cyber Command on cyber conflicts in the globe. The result therefore was in agreement with the research findings of Hoffman (2006) who asserts that the main danger posed by IS does not concern the integrity of countries in the region, but its ability both to channel money and advanced weapons to terror organizations active in the region, and to make the territory under its control, which connects western Iraq with northern and eastern Syria, an impervious haven. The significance of the result caused the null hypotheses to be rejected while the alternative was accepted.

The result of the data analysis in table 2 was significant due to the fact that the calculated R-value (0.94) was greater than the critical R-value (0.113) at 0.05 level with 298 degree of freedom. The result implies that there is significant implication of the operations of ISIS Cyber Command on the global economy. The result of the findings agreed with the findings of World Economic Situation and Prospects (2018) which highlighted that global economy as the economy of the world, considered as the international exchange of goods, has been much affected by cyber crime and other militating forces. The significance of the result caused the null hypotheses to be rejected while the alternative was accepted.

Conclusions

Based on the findings of the research work, it was concluded that there are many cases of operations of ISIS Cyber Command, causing cyber conflicts in the globe. There is significant implication of the operations of ISIS Cyber Command on cyber conflicts in the globe. Finally, the operations of ISIS Cyber Command have negative effects on the global economy.

Recommendations

The following recommendations are deemed necessary:

1. International training courses on countering violent extremism (CVE) should be developed.
2. Open-source intelligence should be gathered by using specialist online surveillance techniques from social networking sites, chat rooms, web sites and Internet bulletin boards.
3. A forum that brings stakeholders from key industrial sectors together to discuss ways to disrupt the IS economy should be created.

REFERENCES

ATC, (2004) Tweeting the Jihad: social media networks of western foreign fighters in Syria and Iraq. *Studies in Conflict & Terrorism*, *38*, 1–22.CrossRefGoogle Scholar

Conway, M. (2003). What is cyber terrorism? The story so far. *Journal of Information Warfare*, *2*(2), 33–42. Google Scholar.

Desmond, P. (2002). Thwarting cyber terrorism. *Network World*, *19*(7), 72–74.Google Scholar

Felson, M. (2002). *Crime and everyday life* (3rd ed.). California:Sage. Google Scholar

Freiburger, T., & Crane, J. 2008. A systematic examination of terrorist use of the internet. *International Journal of Cyber Criminology*, *2*(1), 309–319.Google Scholar

Graham, E. (2017) COULD Isis's cyber Caliphate' unleash a deadly attack on key targets. (online)

Hoffman. H. (2006); *Inside Terrorism*; Columbia University Press. ideology among East German youth. *Political Psychology* 1996: 97-126

Internet, H. (2008). Portrait of rats. *Preparing to Drown. 10th*, (October 2008) Available at: http://internet-haganah.com/harchives/006420.html Accessed 15 Jan 2014.

Jenkins. X. L. (2003) Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind; Johns Hopkins University Press; edited by Walter Reich.

Nickolov, B. M. (2005) Returns to information security investment: the effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information System Front* 8 (5), 339–349.

Philip, X. M. (2016), United Cyber Caliphate published a kill list of 8, 786 individuals in the US, UK.' *Security Affairs,* April 6, 2017.

Powell, B. (2005). Generation Jihad. *Time*, *166*, 56–59.Google Scholar

US Department of Defense, (2012) *Joint Publications 3-13 Information Operations,*. (Online) Available at: http://www.dtic.mil/doctrine/new pubs/jp3 13.pdf (Acessed 11 October 2015).

Wakeford, A. (2015) *Mail and Guardian*. (online) Available at: hyyp://mg.co.za/artice/2015-04-15-state-agency-monitoring-cyberspace-for-isis-recruitment.

World Bank (2011) *Political xenophobia in the transition from socialism:* Threat, racism and war.

World Economic Forum (2015). global cybersecurity index and cyberwellness profiles.(online) avaiable at: hyyp://www:itu. int/drns pub/itu-d/str/d-stsr-secu-2015-pdf (accessed 26 august 2016.)

World Economic Situation and Prospects, (2018) The principal ISIS hacking unit, and other pro-ISIS groups like the Sons Caliphate Army (SCA) and Kalacnikov.TN (KTN) merged and formed The United Cyber Caliphate (UCC)

Zelikow, P. (2003) The Transformation of National Security Five Redefinitions. *The National Interest.*