Cyber Espionage: A Cultural Expression

Dr. Andrew Karamanian
Strategic Security Research
Cisco
Durham, NC, USA
andre377@me.com

Dr. Char Sample
CERT
Carnegie Mellon University
Pittsburgh, PA, USA
csample@cert.org

***Abstract*—Cyber espionage cost the US 508,000 jobs and $24 to $120 billion dollars a year [4]. In addition to the primary loss of intellectual property, several secondary losses are experienced. These secondary losses included: information, which can lead to market manipulations, future innovation opportunities and markets, and reputation losses [4]. A majority of cyber espionage activities appear to support national goals. 87% of cyber espionage campaigns have state sponsorship [8]. This indicates a national priority, and could indicate a type of cultural support for this activity. Kuhn described in his seminal work, "The Structure of Scientific Revolutions" the process of paradigm shifts and their relationship to innovation. Kuhn's suggestion along with Verizon's data appear to support the suggestion that cultures which are readily capable of innovative paradigm shifts may be targeted victims of cyber espionage by cultures that are incapable of the innovative paradigm shifts. This study leveraged Verizon's Data Breach Report containing 511 data points, 470 victim data points, and 230 attacker data points [8]. While this sample was not large enough for a full statistical analysis, the data was sufficient for a pilot study using inferential statistics along with Hofstede's Cultural Dimension Theory. The results inferred a relationship between culture and cyber espionage.**

Keywords—Culture; Cyber Espionage; Hofstede, Spearman Correlation; Mann-Whitney U-Test

I. INTRODUCTION

McConnell, Chertoff, and Lynne [11] publicly stated that the "Chinese government has a national policy of economic espionage in cyber-space." China is not alone, recent events with Russia and Ukraine along with Syria and Iran directing attacks against US interests cyberspace is rapidly emerging as an attack vector that may offer a lower cost of entrance than conventional espionage.

Cyber espionage cost the US 508,000 jobs and $24 to $120 billion dollars a year [4]. In addition to the primary loss of intellectual property, several secondary losses are experienced. These secondary losses included: information which can lead to market manipulations, future innovation opportunities and markets, and reputation losses [4].

A quick examination of the victims and perpetrators revealed that, 87% of cyber espionage campaigns have state sponsorship [8]. The Office of the Director of National Intelligence (ODNI) reported to congress, and a DoD unclassified report on cyber espionage pointed to eastern Europe and Asia [5], [6] as perpetrators of cyber espionage. Specific emphasis has been placed on Russia, Russian speaking eastern European countries, China, and North Korea. The most common victims of this activity were the US, South Korea and Japan [8]. Coincidentally, all three of the victim countries share low to medium power distance (PDI) values while the attacker countries of Russia and China share high PDI values.

The primary goal of cyber espionage is to steal innovative intellectual property [4]. Kuhn [12] identified Innovation as an event occurring when the incremental course of science has run its course, and a paradigm shifts occurs. The possibility exists that cultures which are readily capable of this type of paradigm shift may be targeted victims.

The purpose of this study is to explore the commonality of cultural values for both the victims, and perpetrators of cyber espionage. The study will rely on the data found in the Verizon data breach report, along with Hofstede's cultural dimensions scores [2], [8]. The researchers will perform quantitative inferential analysis using statistical methods in order to examine the common cultural traits of countries involved in the attack.

The Verizon attack data provided 511 data points, however, the number of countries involved in the attack (12 attackeing countries and 9 victim countries) is does not represent an adequate sample size, and this data sample limits the tools that can be used for data evaluation [8]. However, information can still be mined from this data. This study and analysis may provide foundational knowledge for the emerging cross-discipline study of culture and cyber behaviors.

II. GOALS

The researchers for this study seek to explore an answer to the question: does a relationship exist between any cultural dimensions and cyber espionage? Answering this question could provide insight to the benefit to an investment in additional research, funding and access to compiled sensitive data for a full study. Also, should a connection be found, and should such data be obtained, this research may begin to shed light on cyber espionage actor's based on their national culture.

Therefore, the purpose of this study is to explore the relationship between culture and cyber espionage actors, both victims and perpetrators. The study leverages the data found in the Verizon data breach report [8] along with the cultural dimension values that Hofstede makes available to researchers. This study will achieve this purpose through inferential analysis by comparing the Verizon data against of the full population data provided by Hofstede in order to determine the existence of statistically significant findings.

Because the study has identified a small number of countries for the data points of cyber espionage, a full statistical analysis is not possible. The country sample size represents less than 15% of the overall country population, thus the researchers acknowledge the inability to abstract findings to a larger population. However, a simple examination of the cultural profiles of attackers and victims provides potentially useful exploratory information that may help inform future research questions. This analysis can be a first step, and server as a foundation for further study by organizations who seek to analyze their own large private data sets, or a follow-on study should future data become available.

III. Background

Hofstede et al. defined culture across six different dimensions [3]. Each dimension has distinct behaviors and motivations that are scored. The dimensional explanations follow.

- Power Distance (PDI) - Characterized by preferential treatment based on group membership [3]. The low pole of this dimension associates with egalitarian behaviors and the high pole of this dimension associates with authoritarian behaviors [3].
- Individualism Versus Collectivism (IVC) This dimension is characterized by primary consideration of the needs of either self, or the larger societal group first, when making decisions.
- Masculine versus Feminine (M/F) This dimension is characterized by gender roles and the societal response to conflict resolution.
- Uncertainty Avoidance Index (UAI)– This dimension defines a societal response to the unknown from curious, low values, to fearful, high values.
- Long-Term Orientation versus Short-Term Orientation (LTOvSTO). This dimension is characterized on the high end of the pole by "perseverance and thrift" p. 239)[3].
- Indulgence versus Restraint (IVR). This dimension is associated with "enjoying life and having fun" (p. 281) [3].

The dimensional behaviors are not only passed onto societal members, but once these members become adults they can reproduce the cultural values and pass them onto the next generation. Additionally, because cultural behaviors are so strongly re-enforced they become a part of the automatic thought process.

Hofstede et al. addressed innovation in culture dimensions throughout his seminal text [3]. Hofstede et al. identified countries with high uncertainty avoidance as sacrificing innovation for orderliness, and identified the rate of innovation to be slower [3]. Hofestede et al. identified self-actualization and creativity as a trait of countries with high Individualism [3] Guss [9] also confirmed this finding and Yu & Yang [10] in their 2009 study found that collectivism and the "Golden Mean" inhibited creativity. Additionally countries identified as low power distance, tended to have values of adaptability and less concern with alignment with supervisors. These values are arguably necessary for an environment that fosters creativity and innovation. This is not a sufficient condition to be a victim of cyber espionage; however, state sponsored theft of innovation occurs, these traits may appear to be shared by the victims.

TABLE I. Victim Information: Dimensions, Number of Incidents, N Normalized for Country Population of Internet Users [8]

Victims	Hofstede Cultural Dimensions							
	pdi	*Idv*	*mas*	*Ua*	*Lto*	*ivr*	*N*	*Nm*
Viet.	70	20	40	30	57	35	5	1
PhilIpp.	94	32	64	44	27	41	5	1
Belarus	N	N	N	N	81	15	5	5
Colom.	67	13	64	80	13	83	9	1
Ukr.	N	N	N	N	86	14	9	3
Russia	93	39	36	95	81	19	14	1
Japan	54	46	95	92	87	41	19	1
S.Korea	60	18	39	85	100	29	28	3
US	40	91	62	46	25	68	25	5

IV. Population

The countries listed in Table I were taken from the Verizon report and includes the raw data used for victims [8]. Victim data will have the following elements: Country, raw number of hits, number of hits normalized by the country's Internet user population, and Hofstede cultural dimension values. The attacker data illustrated in Table II will display the country and cultural dimension scores. This data includes Russia, China, and Eastern European Russian speaking countries as indicated by Verizon [8]. Hofstede's cultural dimension population for the general population can be obtained at the website geert-hofstede.com.

TABLE II. Actor/Attacker Population [8]

Actors	Hofstede Cultural Dimensions					
	pdi	*idv*	*mas*	*Uai*	*lto*	*Ivr*
EST	40	60	30	60	82.11	16.29
Romania	90	30	42	90	51.88	19.86
Russia	93	39	36	95	81.36	19.86

Actors	**Hofstede Cultural Dimensions**					
	pdi	*idv*	*mas*	*Uai*	*lto*	*Ivr*
China	80	20	66	30	87.40	23.66
Belarus					81	15
Kyrgyzstan					65.99	39.28
Armenia					60.95	
Azerbaijan					60.70	21.65
Moldova					71.03	19.19
Georgia					38.28	31.91
Ukraine					86.39	14.28

V. Method

This study is designed to find an answer to the question: does a relationship exist between any cultural dimensions and cyber espionage principals? Thus, the results of this study will be used to determine common cultural characteristics present in both victims and attackers cyber espionage. Due to the restrictions on the dataset, the researchers relied on two different testing methods when where possible, to determine if there is mutual support across multiple methods of examination. The methods used are the Mann-Whitney U-test and the Spearman correlation. These methods were chosen due to the non-parametric nature of the data.

This study was broken into two sections. The first component was the statistical analysis of the victims cultural dimension values. The second component was the statistical analysis of the attackers cultural dimension values. The statistical analysis used the Mann-Whitney U-test as a comparison of central measures between the test groups and the overall population defined by Hofstede. The Spearman correlation was used to examine the relationship between the number of events and the cultural dimensions, as defined by Hofstede.

There are also effects that may come into play because of the number of users in a country. In order to isolate the effects of country size and user size, the data was normalized by considering the number of Internet users per country. This data was obtained from the website www.internetworldstats.com.

Of the 511 data points available, 470 victim data points, most of which were attributed and 230 attacker data points were available. The countries examined by this study were: Japan, Philippines, Romania, Russia, China, Colombia, Vietnam, Belarus, Kyrgyzstan, Ukraine, Kyrgyzstan, Moldova, Georgia, Azerbaijan, Armenia, United States and South Korea. Precise definitions of countries that were victims were available. Attackers, conversely, were grouped by region, discussed by name in the report, but numbers were not assigned per country. This disparity of data between attackers and victims will affect the analysis.

This study first applied the Mann-Whitney U-test in both cases to compare the population. The victim data was clearly attributed in the report by number of incidents per country. As such, it was also analyzed using Spearman correlational analysis. This provided a way to compare the populations, and perform a correlational analysis.

Consequently, the results for victims had analysis from both Mann-Whitney U-test and Spearman correlation. Where the results were tangible, the second method was examined to determine if there was support of the finding. This study asked does a relationship exist between any cultural dimensions and cyber-espionage? The use of multiple methods corroborating in this exploratory study, may better help answer the question.

The attacker data set had a smaller number of data points. Attribution was regionalized and characterized. Specific actors were acknowledged; however, numbers of attacks per country were not explicitly enumerated. This limited the researchers ability to perform a correlational analysis. Additionally, the Mann-Whitney U-test population analysis could only evaluate presence or absence of a country in the data set. This limits the ability to consider country size, and population frequency. However, this test is an indicator of the existence of a behavior, thus making an inferential analysis possible.

VI. Scope and Limitations

This study will be an exploratory, observational, pilot and capable of providing suggestive results. The data publically available was not sufficient to stand to the rigor of a pure experimental or quantitative study. As such, the acceptable p-values have been relaxed [7] from the normal 0.05 to 0.10. Attacker data, which had fewer data points, is examined using descriptive statistics only via frequency independent Mann-Whitney.

Of Hofstede's 100 countries profiled, this study examined attacker profiles of 11 countries [2]. These countries were referred to as China, North Korea, Russia and Russian speaking Eastern Europe [8]. Of these several partial cultural profiles available via cultural dimension theory and no data existed for North Korea.

Another significant limitation is the researcher's cultural bias. The researchers are nationals of the primary victim identified in the study. The researchers have attempted to maintain an observational and objective approach; however, the cultural value systems native to the researches, regardless of individual bias, should be noted.

VII. Results

A. *Victim Observations*

Tables III and IV present the results of a Spearman correlation, r-score, with consideration of Cohen's evaluation of correlation strength, and the accompanying t-value [1]. Also included in Table III are the Mann-Whitney U-test results for the Z-score and the p-value. When a result is identified with supporting corroboration; that result is commented upon.

B. Attacker Observations

The number of data points available for this sample was 230. The size of the sample was smaller by 100% in comparison to the victim data. Additionally, the description available in the Verizon report on the actors was not as detailed [8]. Rather than exclude any analysis on attackers, the choice was made to perform provide descriptive statistics comparing zthe group of actors to the population at large. The examination considered the Z-scores of the actors with the Hofstede control group, for any statistically significant findings [2]. The Z-scores and p-values from the Mann-Whitney U-test analysis appear in Table IV. Table V illustrates the Z-scores based on the attacker shift away from the broader population.

TABLE III. MANN-WHITNEY Z-SCORE AND P, SPEARMAN CORRELATION AND T-SCORE OF CYBER ESPIONAGE VICTIMS

Victims	**Mann-Whitney Results and Spearman Correlation**				
	p $_{(1)}$	***p*** $_{(2)}$	***Z-Score***	***Rs***	***t (rs)***
PDI	0.090	0.180	-1.34	-0.642	-1.88
IDV	0.171	0.342	0.95	0.1071	0.24
MAS	0.161	0.322	0.99	-0.198	-0.45
UAI	0.363	0.726	-0.35	0.3571	0.85
LTO	0.049	0.098	1.65	0.1087	0.29
IvR	0.013	0.027	-2.21	-0.242	-0.66

TABLE IV. ILLUSTRATES MANN-WHITNEY RESULTS WHEN COMPARING WITH THE SPEARMAN CORRELATION

Victim	**Mann-Whitney and Z-score & Spearman Correlation**		
	Z-score	***r*** $_{(s)}$	***Cultural Dimension Statistical Significance***
PDI	-1.34	-0.642	Strongly Suggestive Strong r$_{(s)}$, supporting Z indicator
IDV	0.95	0.107	
MAS	0.99	-0.198	
UAI	-0.35	0.357	
LTO	1.65	0.108	Suggestive Near statistical significance
IvR	-2.21	-0.242	Strongly Suggestive Strong Z significance, weak rs support

TABLE V. ILLUSTRATES THE Z-SCORES BASED ON THE ATTACKER SHIFT AWAY FROM THE BROADER POPULATION

Attacker	**Mann Whitney Results Attackers**			
	Z- Score	***p*** $_{(1)}$	***p*** $_{(2)}$	***Significance***
PDI	1.24609	0.112	0.212	Insufficient
IDV	-0.17923	0.428	0.857	Insufficient
MAS	0.699	0.484	0.242	Insufficient
UAI	0.648	0.516	0.2582	
LTO	3.37	.0004	.0008	Strongly Suggestive
IvR	-3.55	.0002	.0004	Strongly Suggestive

The populations were placed side by side in order to have a visual queue of the population distributions indicated in the results. The Fig. 1-3 illustrate the populations for actors based on PDI, LTO and IVR.

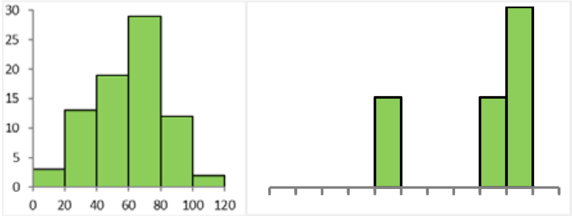

Fig. 1. Illustrates the distribution of PDI when considering the control distribution and the population of actors with the control, i.e. Hofestede, (left) vs. Actors (right)

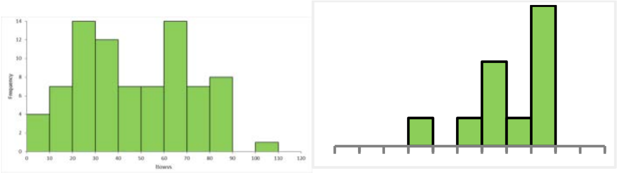

Fig. 2. Illustrates the distribution of LTO when considering the control distribution and the population of actors with the control, i.e. Hofestede, (left) vs. Actors (right)

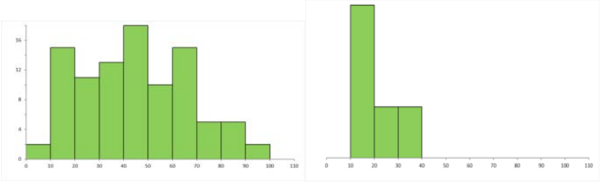

Fig. 3. Illustrates the distribution of IVR when considering the control distribution and the population of actors with the control, i.e. Hofestede, (left) vs. Actors (right).

VIII. ANALYSIS AND CONCLUSIONS

A. Victims

The most significant finding was for IVR. The Mann-Whitney U-test pointed to a statistically significant finding for restraint, with moderate support from Spearman correlation, suggesting activity in this dimension. A restrained culture tends to suppress gratification [3]. This type of denial of gratification, depending on the type of gratification, may result in funneling energy into other pursuits. When cyber espionage activities are encouraged by those in power the possibility exists that hacking becomes a fun pursuit with a creative outlet. Further study is required to address how this dimension may affect the dynamics of both victims and attackers.

PDI produced a "strong" correlation and a Z-score with p-value that while not statistically significant, of potential interest. However, due to the small sample size and the volatile nature of this data this finding will require follow-on research. This finding appears to raise a question about victimology associated with low PDI targets. These societies are known for egalitarian values, and individual empowerment [3]. These societies, often times, accompany higher IDV scores [3]. In this study the high number of attacks against the US may have skewed the results or could indicate a potential emerging victim profile. A follow-on study with a larger data set will ultimately provide greater insight to this issue.

B. *Atackers*

The results were descriptive and examined the relative populations between the Hofstede group, which represents the general world population, and the espionage actor group. Three results were observed. The dimensions that suggested relevant findings were for high power distance, long-term orientation, and restraint. However, because the attacker group only had four entries for pdi, ivc, mas and uai there are no available findings for these dimensions with attackers. The remaining two dimensions had a slightly larger data set so some analysis was performed.

Long-term orientation and restraint had strongly suggestive results. This suggests a patient culture, which is willing to wait to achieve a result [3]. Restrained cultures tend to not want to be in the spotlight, so they are adapt at minimizing their visibility [3]. Espionage in general is not an act that is known for seeking attention. Hofstede et al. [3] observed the attention seeking behavior associated with indulgent cultures along with the uncomfortable response to attention in the restrained cultures. The connection between cyber espionage, long term orientation and restraint is suggestive of advanced persistent threats, which are often executed low (without calling attention to oneself consistent with restraint) and slow (LTO). While China has historically been associated with the Advanced Persistent Threat, the findings of restraint and long-term orientation also reflect the values of other countries that share China's dimensional values and appear to support cyber espionage.

IX. Summary and Future Research

This was an exploratory, observational, pilot study. This study was designed to explore indications of a connection between cyber espionage and culture. The study explored the actors and victims of cyber espionage.

Among the victims, the study identified three possible cultural dimensions that merit further investigation. The suggestion of a connection between for low PDI, LTO and IVR (restraint) were present.

Among the attackers, the study also identified three possible cultural dimensions of potential interest. These were high power distance, long-term orientation and indulgence versus restraint. However, this data set had significantly fewer points than the victim data set, and further investigation could determine if the results from this study were suggestive of a phenomena or simply a random finding.

Future research is heavily dependent on the retrieval of additional data, some of which is likely not readily available. The data may be plausibly obtainable. This area of research and the techniques used suggests that a cross-discipline approach to threat intelligence may provide additional insights into other areas of cyber-security.

References

[1] J. Cohen, (1988). "Statistical Power Analysis for the Behavioral Sciences 2nd Edition," Lawrence Erlbaum Associates, Publishers: New York, NY.

[2] "Geert Hofstede-institute website," (2013). Retrieved from http://www.geert-hofstede.com.

[3] G. Hofstede, G. J. Hofstede, and M. Minkov, (2010). "Cultures and Organizations," McGraw-Hill Publishing: New York, NY.K. Elissa,

[4] McAfee, (2013). "Economic Impact of Cybercrime," Retrieved from http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

[5] Office of the Director of National Intelligence, Counterintelligence Executive, (2011). "Report to Congress on Foreign Economic CoIlection and Industrial Espionage," Retrieved from http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

[6] Office of the Secretary of Defense (2013). "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013," Retrieved from http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf

[7] University of New England (2000). "Inferential Statistics," Retrieved from http://webstat.une.edu.au/unit_materials/c5_inferential_statistics/what_alpha_level.html

[8] VERIZON, (2014). "Data Breach Investigations Report," Retrieved from http://www.verizonenterprise.com/DBIR/2014/

[9] Guss, C. D. (2011). "Fire and ice: Testing a model on culture and complex problem solving," Journal of Cross-Cultural Psychology, 42(7), pp. 1279 – 1298. doi: 10.1177/0022022110383320

[10] Y. Yu and Q. Yang, (2009). "An analysis of the impact Chinese and western cultural values have on technological innovation," Second International Workshop on Knowledge Discovery and Data Mining, Jan 23-25, 2009, pp. 460-463 doi: 10.1109/WKDD.2009.149

[11] M. McConnell, M. Chertoff, and W. Lynn, (2012), "China's Cyber Thievery is National Policy – And Must be Challenged," Wall Street Journal. Available: http://online.wsj.com/news/articles/SB10001424052970203718504577178832338032176#printMode

[12] T. S. Kuhn, (2012), "The Structure of Science Revolutions: 50th Anniversary Edition," University of Chicago Press.