Cultural Markers in Attack Attribution

Char Sample

44CON 2013

Introduction

- Char Sample
  - D. Sc. IA, Culture in CNA Behaviors
  - CERT
  - Defended April 18, 2013
  - Acknowledgements
    - Dave Barnett
    - Maurice Smit
    - Dr. William Kight
    - Dr. Dana LaFon
    - Dr. Dominick Guess

What Are We Really Trying to Accomplish?

- Attribution … and other things.
  - A way around the cat and mouse game of IP address and anonymizers.
  - Perhaps ways to cloak ourselves.
  - Ways to discover new weaknesses or blind spots in ourselves and our adversaries.
- A way to ***quantitatively*** prove the above!
- The real long-term goal.

What Are We Looking For?

FINDING A
IN A
= SUCCESS!!

The Reality Is…

The Research Goal

Applying New Methods to Old Problems

- Can we use other methods such as thought processes to source an attack?
- Is this a valid approach?

A Different Thought

- What if attackers unknowingly left clues or behavior based evidence?

Why This Approach

- Haven’t we tried this before???
  - No, we tried psychological profiling and that had mixed results.
  - Culture is a unique way to look at the problem.
    - Cultural studies are not very old.
    - Cultural studies in other disciplines have been very successful.
    - Cultural studies are easy for techies to understand.

Refining the Thought

- What if the evidence was influenced by culture?
- How does culture influence thought?
- How does a researcher prove all of this?

Start with Thought

- Conscious thought 40-60 bps.
- Unconscious thought 11, 200,000 bps.

"On the Internet, nobody knows you're a dog."

What About Culture?

- Hofstede, Hofstede & Minkov
  - Definition of culture: "the collective mental programming of the human mind which distinguishes one group of people from another".

What About Culture?

- Dr. Dominick Guess
  - – Culture influences problem perception, strategy development and the decision choices.

How is Culture Learned?

- Family
- Small societal groups
- Education
  - Cognition
  - Technology usage
- Greater Society

Learning Culture

- Bargh and Morsella (2008):
  - “Cultural norms and values are readily absorbed during the early phase of life; behaviors and values of those closest to us are also absorbed”.
  - “Culture appears to permeate both unconscious thought and conscious thought”.

Learning Culture

- Gifford (2005) - Past events help to form future perceptions. (Bayesian belief process).
  - A common example of Bayesian belief process

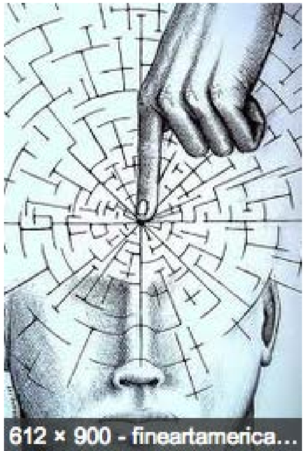
CLICK TO CONTINUE

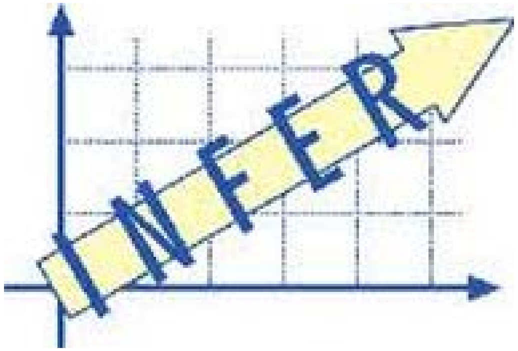
Problem Statement

- The problem is the lack (or absence) of quantitative literature that supports or refutes the role of culture in CNAs.
- The research results must illustrate if a relationship between culture and CNAs exists.
  - The Internet unifies us, won't there be one single techie culture? Cultural convergence? (Clarke, 2004)
  - Why study attacks by country?

Purpose Statement

- Determine, through inference, if a relationship exists between culture and CNA behaviors.
  - Use existing data for test and control groups.
  - Data is also publicly available.
  - Inference vs correlation or causation.



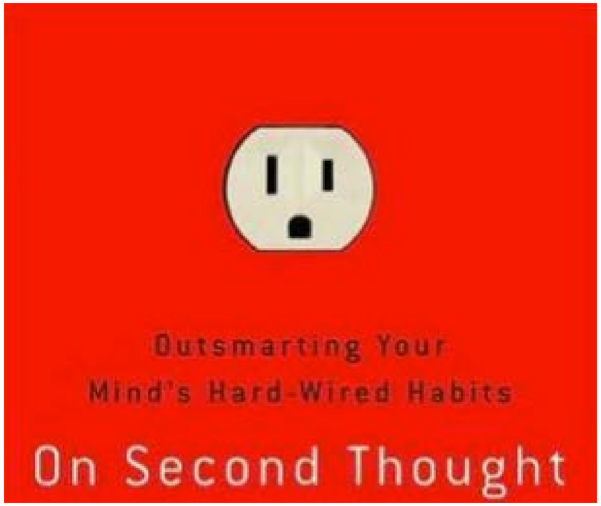


Literature Review

- Baumeister & Masicampo, 2010; Evans, 2008
  - The influencing role of culture in thought is pervasive.
  - The influence of culture in cognition is inescapable and *habitual*.
- Hofstede, Hofstede, & Minkov 2010; Minkov, 2013
  - Unlearning habits or automatic thought processing is more difficult than learning the behavior.
  - Easier to learn and absorb cultural norms than to unlearn them.

The Role of Culture

- Buchtel & Norenzayan (2008)
  - “The cultural differences are best conceptualized ***as differences in habits of thought***, rather than differences in the actual availability of information processing”.



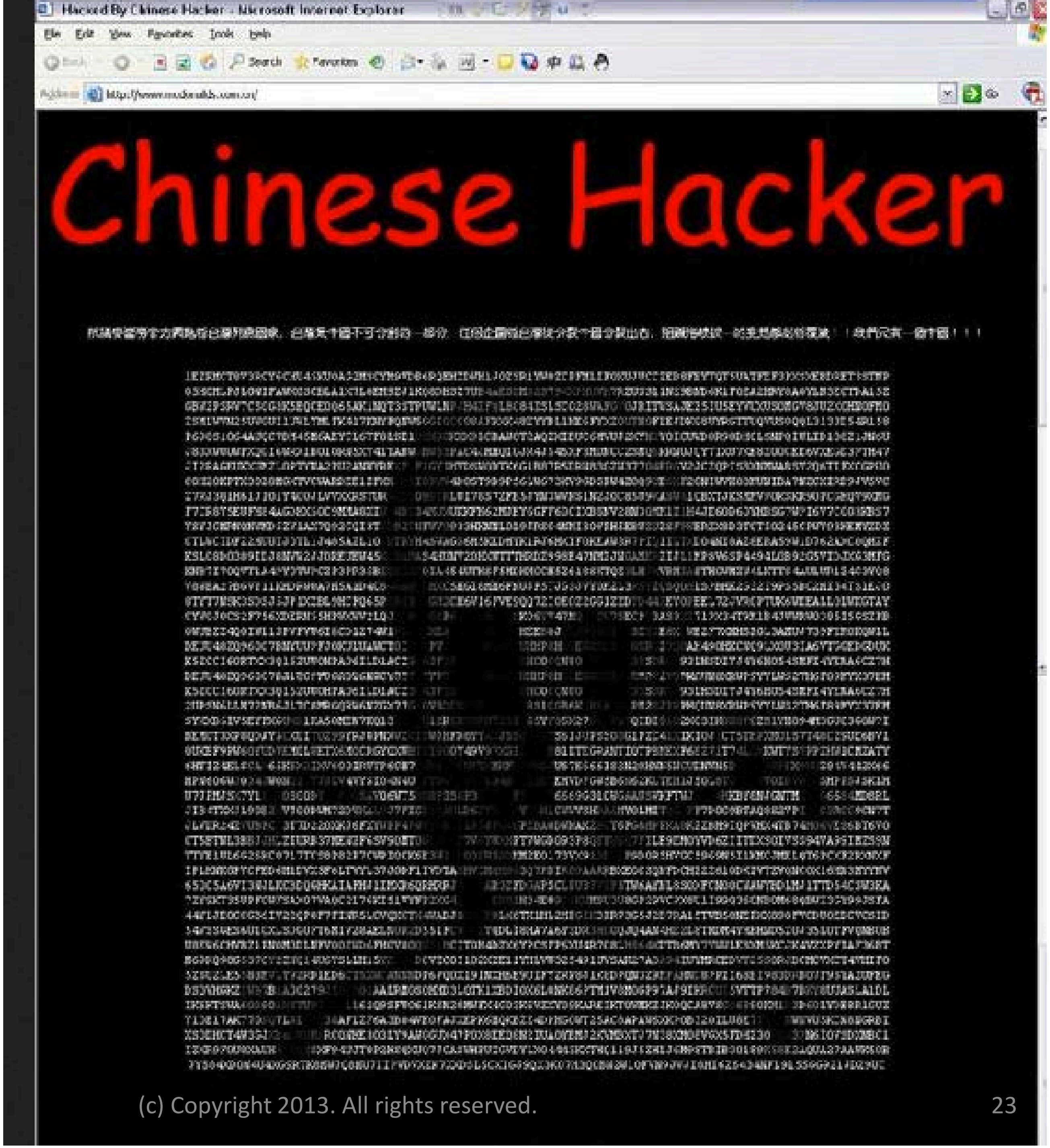
Literature Review Cultural Dimensions

- Hofstede identified 4 cultural dimensions:
  - Power distance (pdi)
  - Individualism vs Collectivism (ivc)
  - Masculine vs feminine (m/f)
  - Uncertainty avoidance (uai)
- Others have added to the model
  - Long Term Orientation(vs Short Term Orientation (ltovsto) - Bond
  - Indulgence vs restraint (ivr) - Minkov

Cultural Dimensions & Attacks

- Power Distance (PDI) – (11-104)
  - Egalitarian vs Bureaucratic - “Beg forgiveness” vs ask permission”. Where does power originate?

China
pdi 80
idv 20
m/f 66
ua 30
ltovssto 87
idr 24

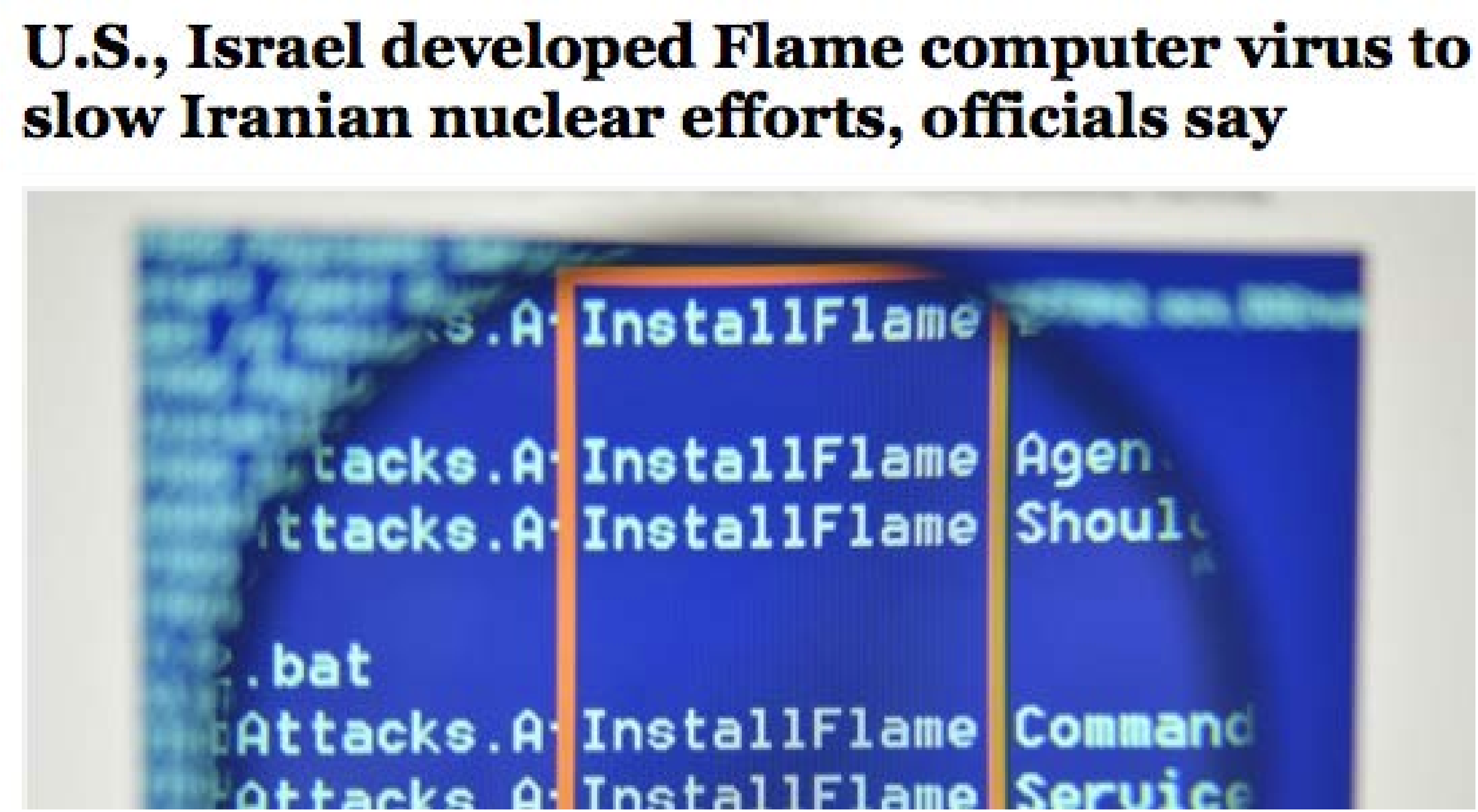

Hacked By Chinese Hacker - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.mcdonalds.com.cn/
Go
Chinese Hacker
[illegible] 我們只有一個中國！！！

Cultural Dimensions & Attacks

- Individualism vs Collectivism (IVC) – (6-91)
  - “I am in charge of my own destiny” vs “The needs of the group must first be considered”.
  - Education
    - Individual: *“How to learn”*
    - Collectivist: *“How to do”*

I Respect ©
We Respect

Washington Post



U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say

```
s.A InstallFlame
tacks.A InstallFlame Agen
ttacks.A InstallFlame Shoul
.bat
Attacks.A InstallFlame Command
Attacks.A InstallFlame Service
```

Profiles of Israel and US

- Israel
  - *pdi: 13*
  - ***idv: 54***
  - m/f: 47
  - ua: 81
  - ltovssto: 36
  - ivr: n/a

- US:
  - pdi: 40
  - ***idv: 91***
  - m/f: 62
  - ua: 46
  - ltovssto: 26
  - ivr: 68

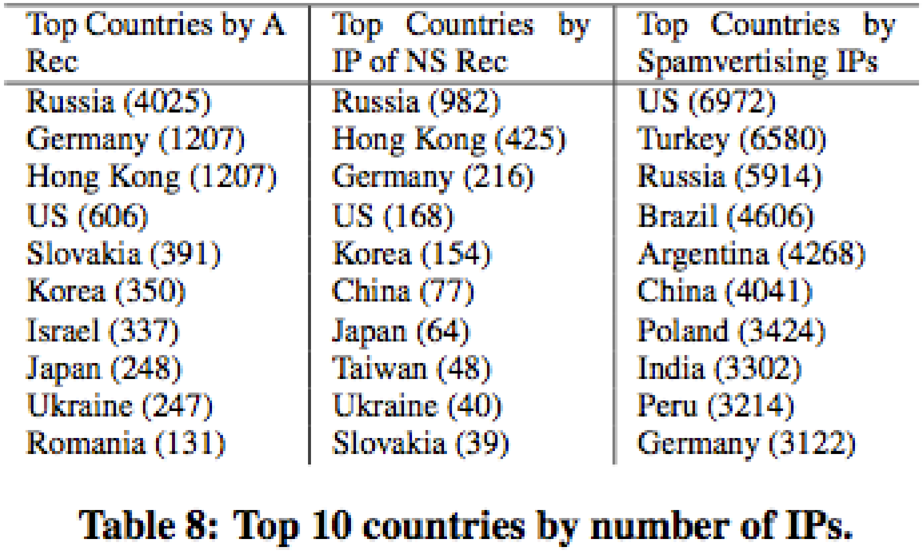
Cultural Dimensions & Attacks

- Masculine vs Feminine (M/F) – (5-110)
  - – Aggression vs consensus

    “Give him an inch and he’ll take a mile” vs “Let’s negotiate”.

Fast Flux DNS

(Konte, Feamster & Jung, 2008)

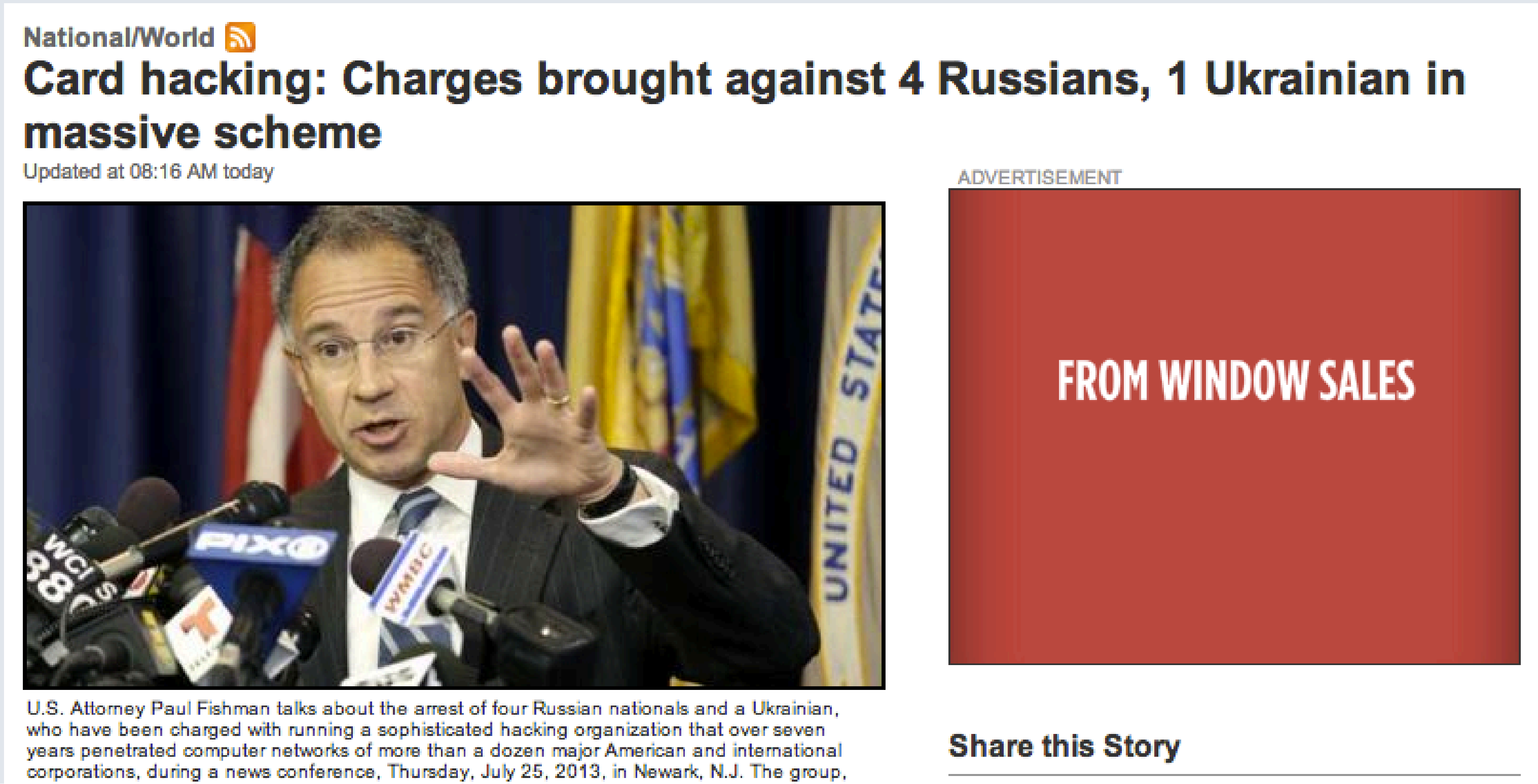


Top Countries by A Rec	Top Countries by IP of NS Rec	Top Countries by Spamvertising IPs
Russia (4025)	Russia (982)	US (6972)
Germany (1207)	Hong Kong (425)	Turkey (6580)
Hong Kong (1207)	Germany (216)	Russia (5914)
US (606)	US (168)	Brazil (4606)
Slovakia (391)	Korea (154)	Argentina (4268)
Korea (350)	China (77)	China (4041)
Israel (337)	Japan (64)	Poland (3424)
Japan (248)	Taiwan (48)	India (3302)
Ukraine (247)	Ukraine (40)	Peru (3214)
Romania (131)	Slovakia (39)	Germany (3122)

Table 8: Top 10 countries by number of IPs.

Russia
pdi 93
idv 39
m/f 36
ua 95
ltovssto 81
idr 20

Non-Confrontational Crimes



National/World

Card hacking: Charges brought against 4 Russians, 1 Ukrainian in massive scheme

Updated at 08:16 AM today

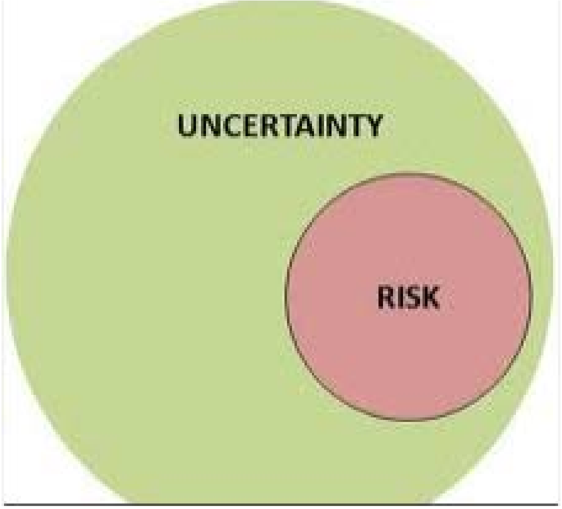
U.S. Attorney Paul Fishman talks about the arrest of four Russian nationals and a Ukrainian, who have been charged with running a sophisticated hacking organization that over seven years penetrated computer networks of more than a dozen major American and international corporations, during a news conference, Thursday, July 25, 2013, in Newark, N.J. The group,

Share this Story

Cultural Dimensions & Attacks

- Uncertainty Avoidance (UAI) – (8-112)
  - How a society deals with the unknown.

    Threatened & uncomfortable with ambiguous situations vs curious about the unknown.



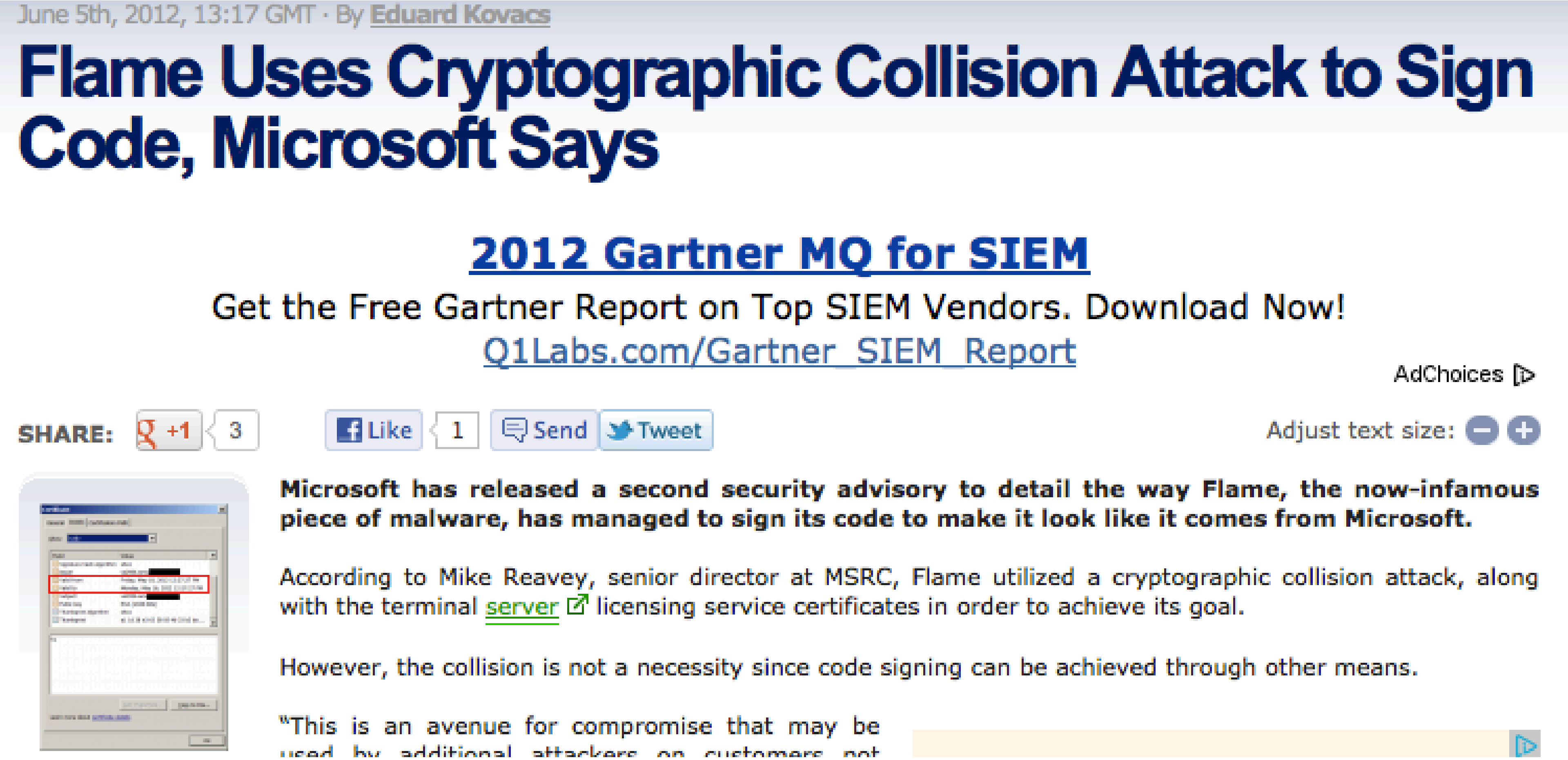
Google Disrupts Chinese Spear-Phishing Attack on Senior U.S. Officials

BY KEVIN POULSEN 06.01.11 6:28 PM

Comparison China vs US (both low on UA)

- China
  - pdi 80
  - idv 20
  - m/f 66
  - ***ua 30***
  - ltovssto 87
  - idr 24

- US
  - pdi 40
  - Idv 91
  - m/f 62
  - ***ua 46***
  - ltovssto 26
  - idr 68



June 5th, 2012, 13:17 GMT · By Eduard Kovacs

Flame Uses Cryptographic Collision Attack to Sign Code, Microsoft Says

Microsoft has released a second security advisory to detail the way Flame, the now-infamous piece of malware, has managed to sign its code to make it look like it comes from Microsoft.

According to Mike Reavey, senior director at MSRC, Flame utilized a cryptographic collision attack, along with the terminal server licensing service certificates in order to achieve its goal.

However, the collision is not a necessity since code signing can be achieved through other means.

"This is an avenue for compromise that may be used by additional attackers on customers not

Comparison China vs US (both low on UA)

- US
  - pdi 40
  - idv 91
  - m/f 62
  - ***uai 46***
  - ltovssto 26
  - ivr 68

- Israel
  - pdi 13
  - idv 54
  - m/f 47
  - ***uai 81***
  - ltovssto 38
  - ivr n/a

Cultural Dimensions & Attacks

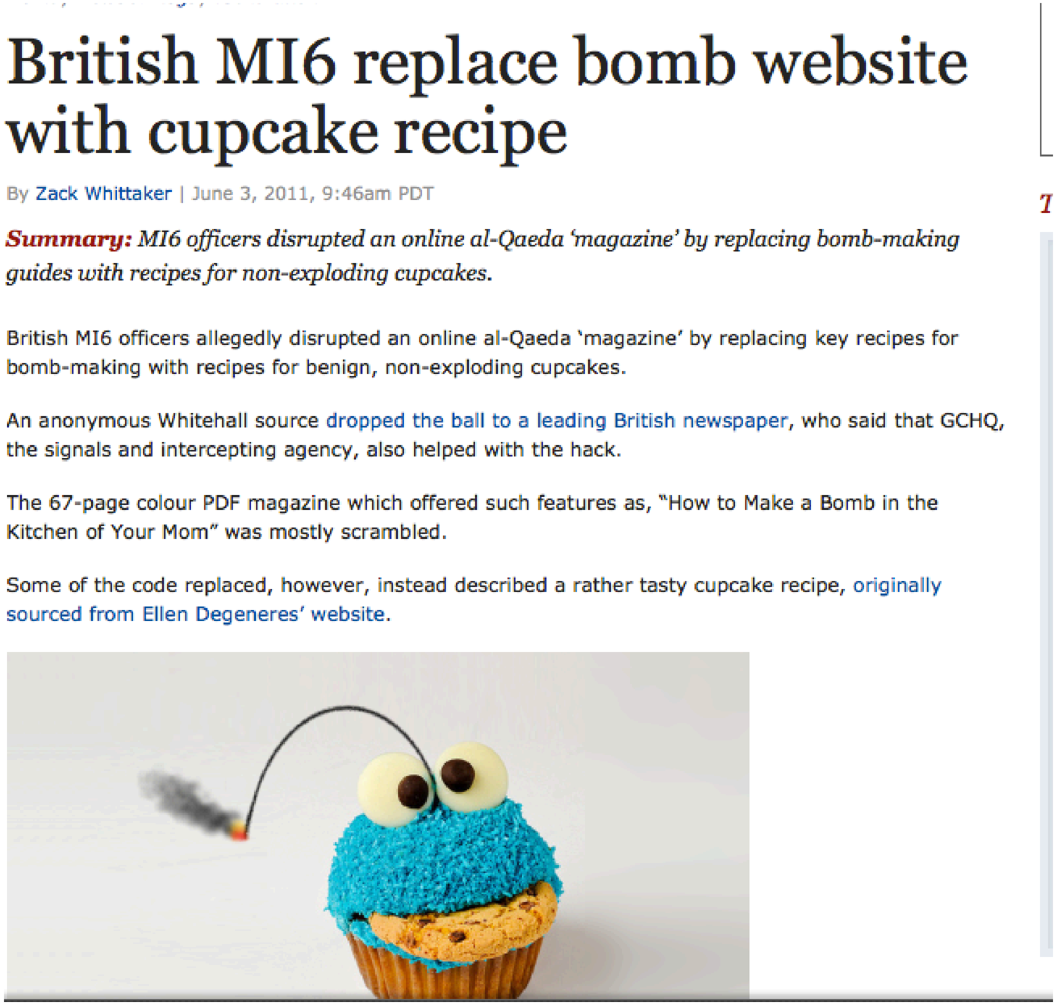
- LTO vs STO – (0-100)
  - LTO: Fosters virtues aimed at future rewards
    - Characterized by perseverance & hard work.
    - Thrifty, but will invest.
  - STO: Fosters virtues aimed at past and present
    - Characterized by crediting luck.
    - Will use “risky” behaviors.

Cultural Dimensions & Attacks

- Indulgence vs Restraint (IVR) – (0-100)
  - Free gratification vs restraint.
    - Indulgent: enjoy life, have fun, appreciate compliments, positive outlook.
    - Restraint: moderation, "disinterested and pure", few desires, suspicious or embarrassed by compliments, negative outlook.

Indulgence vs Restraint

UK
pdi 35
idv 89
m/f 66
ua 35
ltovssto 51
ivr 69



British MI6 replace bomb website with cupcake recipe

By Zack Whittaker | June 3, 2011, 9:46am PDT

Summary: *MI6 officers disrupted an online al-Qaeda 'magazine' by replacing bomb-making guides with recipes for non-exploding cupcakes.*

British MI6 officers allegedly disrupted an online al-Qaeda 'magazine' by replacing key recipes for bomb-making with recipes for benign, non-exploding cupcakes.

An anonymous Whitehall source dropped the ball to a leading British newspaper, who said that GCHQ, the signals and intercepting agency, also helped with the hack.

The 67-page colour PDF magazine which offered such features as, "How to Make a Bomb in the Kitchen of Your Mom" was mostly scrambled.

Some of the code replaced, however, instead described a rather tasty cupcake recipe, originally sourced from Ellen Degeneres' website.

US
pdi 40
idv 91
m/f 62
ua46
ltovssto 26
ivr 68

Variables

- Independent variable
  - – Culture
  - – Six dimensions defined by Hofstede et al. (2010)
    - PDI (11-104)
    - IVC (6-91)
    - M/F (5-110)
    - UAI (8-112)
    - LTO (0-100)
    - IVR (0-100)
- Dependent variable: CNA behaviors

Research Questions

- Research Questions:
  - **RQ1:** Does a relationship exist between high power distance index values **or** any other cultural dimensional values and nationalistic, patriotic themed website defacements?
    - Success relies on truth table results
    - The role of "***or***"

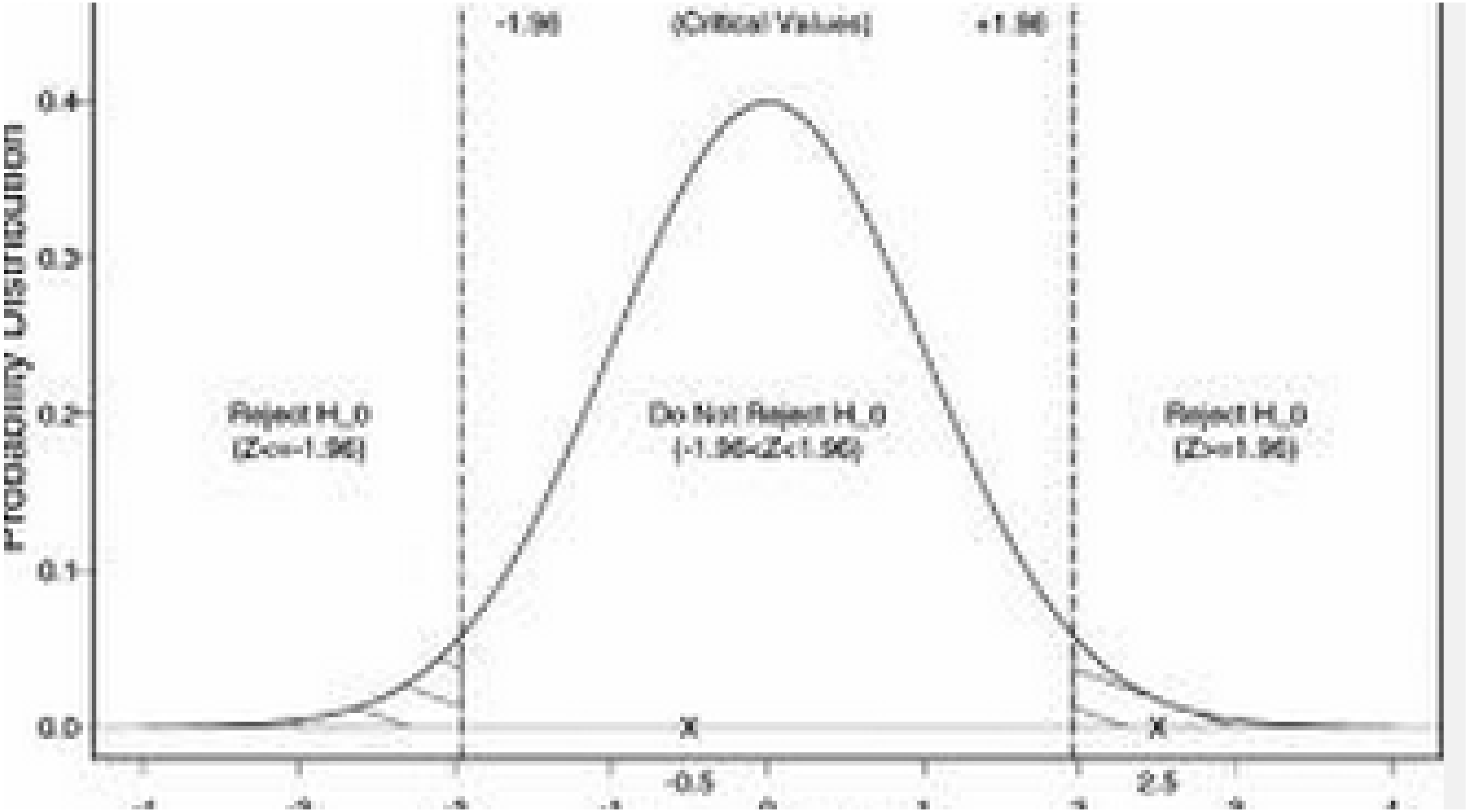
Hypothesis

- Hypothesis
  - A relationship exists between culture and CNA behaviors.
    - H_0 There is no relationship between culture and CNA behaviors.
    - H_1 A relationship exists between culture and CNA behaviors.
  - Hypothesis further decomposed into more specific tests, same question posed for each dimension.

Research Plan (1)

- Quasi-experiment comparing a non-random sample against the overall population.
  - Research question 1: Extract countries of origin from reports of nationalistic, patriotic themed website defacements for comparison against Hofstede’s data on countries.
    - Compare scores to Hofstede’s operationalized data.
    - Compare using measurements of central tendency.
    - Hypothesis Tests:
      - $H1_0$: There is no relationship between high PDI values or any other dimensional values and nationalistic, patriotic themed website defacements.
      - $H1_{1\text{-}6}$: A relationship exists between dimensional value and nationalistic, patriotic themed website defacements.

Hypothesis Testing



Issues, Concerns, Caveats

- Issues, concerns, caveats, etc.
  - “The study of culture and decision making is a relatively new and unexplored field (Guss, 2004).”
  - Must guard against stereotypes.
  - Hofstede’s work is not as precise as some would like but it does offer quantifiable data that is periodically updated.
  - Even the obvious, must be supported by data.

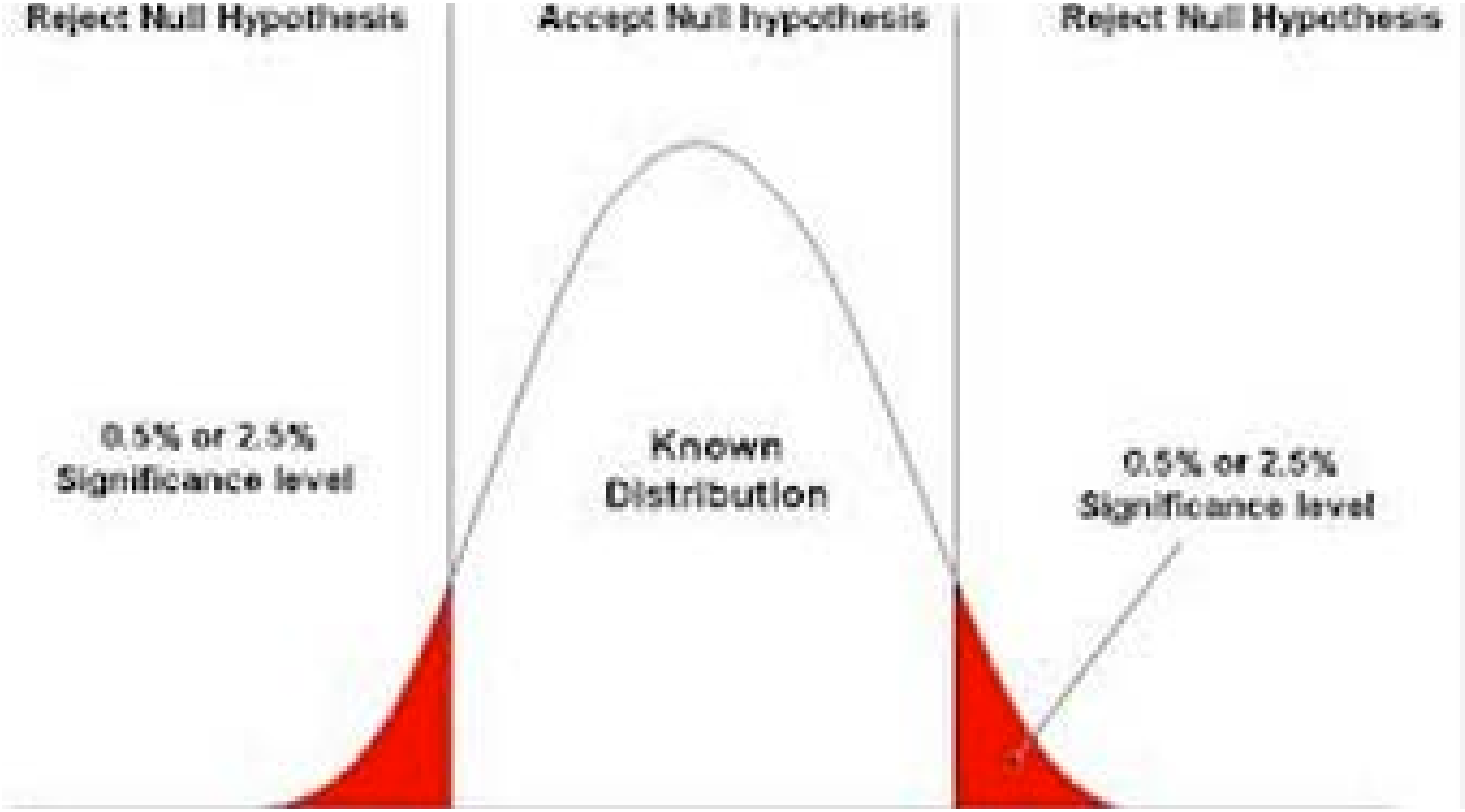
Data Collected: Dataset

- Searched on nationalistic, patriotic themed attacks.
  - Verified results through peer reviewed academic studies.
  - Nominal scoring:
    - Studies were qualitative so an accurate count was not possible.
    - Country is scored if verified evidence exists that shows that the country participated in nationalistic, patriotic themed attacks.
  - Collected data on the following countries:
    - Bangladesh, China, India, Indonesia, Iran, Israel*, Malaysia, Pakistan, Philippines, Portugal, Russia, Singapore, Taiwan, and Turkey. (Columbia, Brazil, and Morocco were dropped due to lack of verifying studies or reports in English.)
      - The special case of Israel.
      - The follow on search.
- Means tested the results.

Rules for Success

- In order to reject the null hypothesis, a resulting value for p* must be <= 0.05.
  - This means that if a random sample were drawn, the likelihood of getting these results would be 5%.
  - The lower the value the more plausible the alternative hypothesis.
  - Put another way, results are in the tail of the normal distribution curve.

Hypothesis Testing



RESEARCH QUESTION #1

Results (1) – Peer Reviewed Data

Results of Research Question One Tests

Hypothesis #	Test	Tool	Z=	p-value	Accept/Reject
(PDI) $H1_{0,}$ $H1_1$	μ <= 59	Mann-Whitney	**1.91**	**0.0281**	**Reject**
(IVC) $H1_{0,}$ $H1_2$	μ >=45	Mann-Whitney	**-2.17**	**0.015**	**Reject**
(M/F) $H1_{0,}$ $H1_3$	μ <= 50	Mann-Whitney	0.5753	0.4247	Accept
(UAI) $H1_{0,}$ $H1_4$	μ <= 68	Mann-Whitney	-1.16	0.123	Accept
(LTO) $H1_{0,}$ $H1_5$	μ <= 45	Mann-Whitney	1.15	0.1251	Accept
(IVR) $H1_{0,}$$H1_6$	μ >= 45	Mann-Whitney	-1.51	0.0655	Accept

Results (1) – All Data

Results of Research Question One Tests

Hypothesis #	Test	Tool	Z=	p-value	Accept/Reject
(PDI) $H1_{0,}$ $H1_{1}$	μ <= 59	Mann-Whitney	**2.08**	**0.0188**	**Reject**
(IVC) $H1_{0,}$ $H1_{2}$	μ >=45	Mann-Whitney	**-2.3**	**0.0107**	**Reject**
(M/F) $H1_{0,}$ $H1_{3}$	μ <= 50	Mann-Whitney	0.16	0.4364	Accept
(UAI) $H1_{0,}$ $H1_{4}$	μ <= 68	Mann-Whitney	0.9	0.1841	Accept
(LTO) $H1_{0,}$ $H1_{5}$	μ <= 45	Mann-Whitney	-0.31	0.3783	Accept
(IVR) $H1_{0,}$$H1_{6}$	μ >= 45	Mann-Whitney	0.74	0.2297	Accept

Results (1) – Peer Reviewed Data

Results of Question One Test Without Israel

Hypothesis #	Test	Tool	Z=	p-value	Accept/Reject
(PDI) $H1_{0,}$ $H1_1$	μ <= 59	Mann-Whitney	**2.42**	**0.0078**	**Reject**
(IVC) $H1_{0,}$ $H1_2$	μ >= 45	Mann-Whitney	**-2.35**	**0.0094**	**Reject**
(M/F) $H1_{0,}$ $H1_3$	μ >= 50	Mann-Whitney	0.5714	0.4247	Accept
(UAI) $H1_{0,}$ $H1_4$	μ <= 68	Mann-Whitney	-1.33	0.0918	Accept
(LTO) $H1_{0,}$ $H1_5$	μ <= 45	Mann-Whitney	1.15	0.1251	Accept
(IVR) $H1_{0,}$ $H1_6$	μ >= 45	Mann-Whitney	- 1.51	0.0655	Accept

Results (1) – All Data

Results of Research Question One Tests without Israel

Hypothesis #	Test	Tool	Z=	p-value	Accept/Reject
(PDI) $H1_{0,}$ $H1_1$	$\mu <= 59$	Mann-Whitney	**2.54**	**0.0055**	**Reject**
(IVC) $H1_{0,}$ $H1_2$	$\mu >=45$	Mann-Whitney	**-2.45**	**0.0071**	**Reject**
(M/F) $H1_{0,}$ $H1_3$	$\mu <= 50$	Mann-Whitney	- 0.19	0.4247	Accept
(UAI) $H1_{0,}$ $H1_4$	$\mu <= 68$	Mann-Whitney	1.04	0.1492	Accept
(LTO) $H1_{0,}$ $H1_5$	$\mu <= 45$	Mann-Whitney	-0.35	0.3632	Accept
(IVR) $H1_{0,}H1_6$	$\mu >= 45$	Mann-Whitney	0.74	0.2297	Accept

Results (1)

Truth Table Results for Research Question One

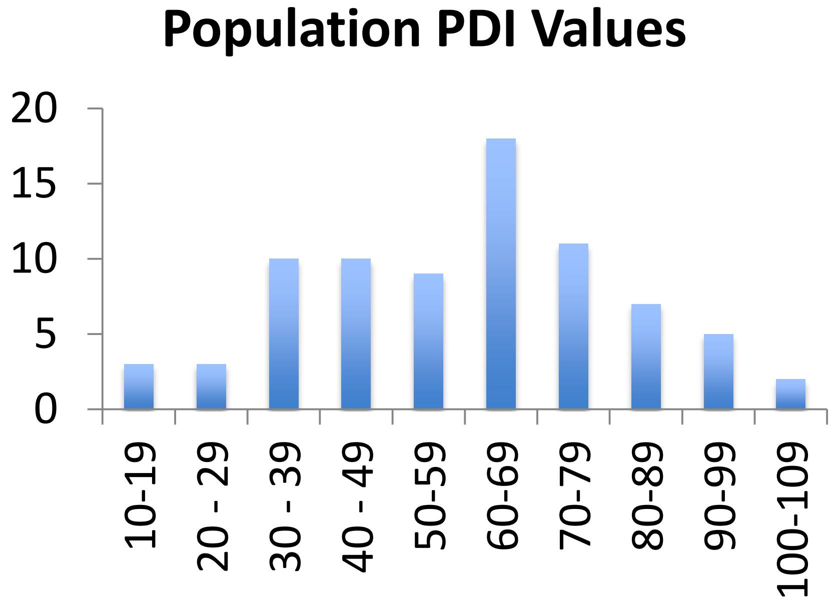
PDI	IVC	M/F	UAI	LTOvSTO	IVR
1	1	0	0	0	0

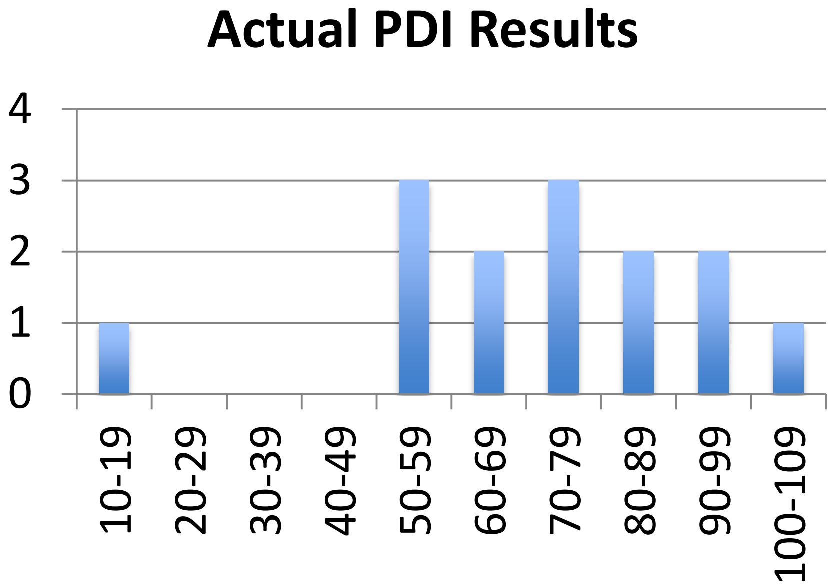
Note. 0 indicates the null hypothesis was accepted for the dimensional question and 1 indicates that the null hypothesis was rejected.

Results – PDI (Useable Data)

Control Data

Sample Data

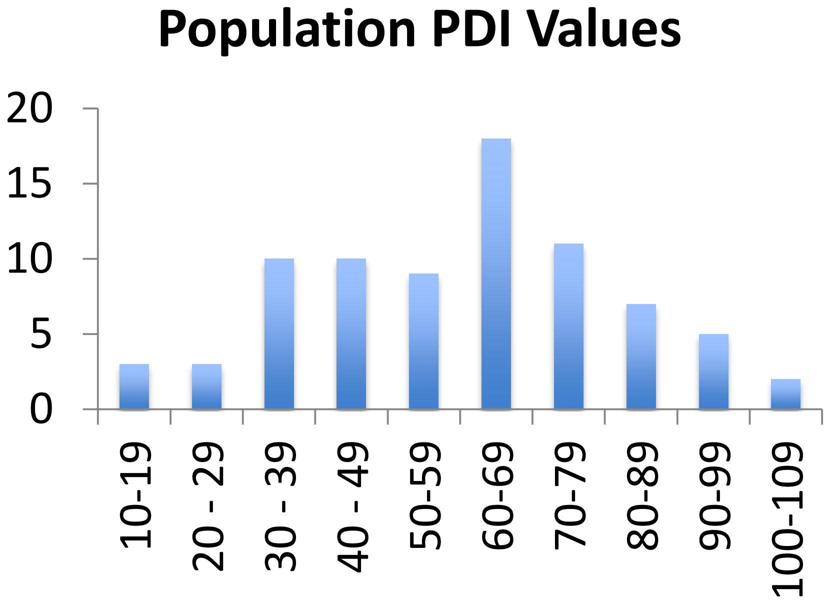




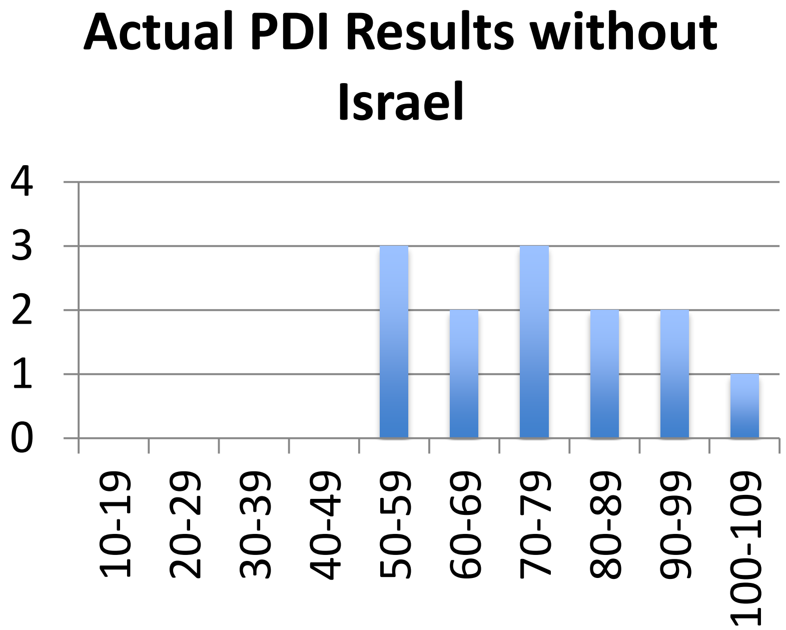
Results – PDI (Useable Data – IL)

Control Data

Sample Data



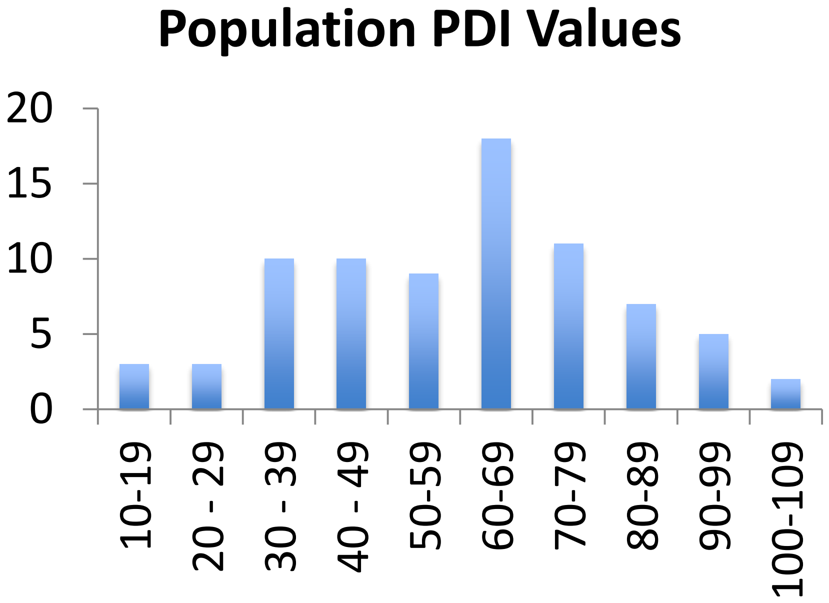
Population PDI Values



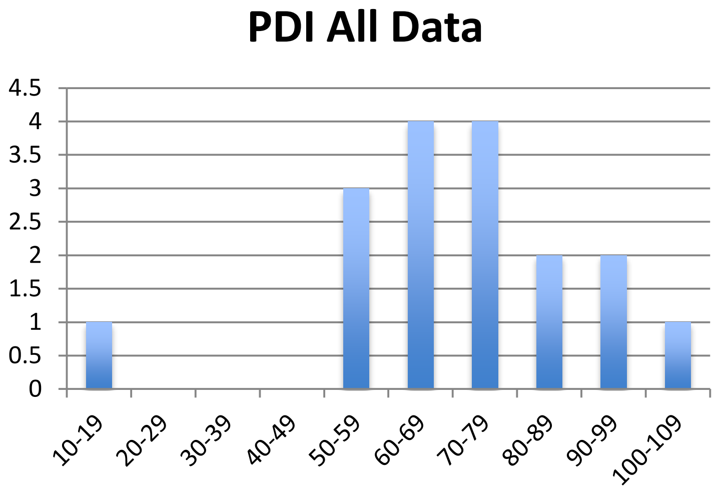
Actual PDI Results without Israel

Results – PDI All Data

Control Data



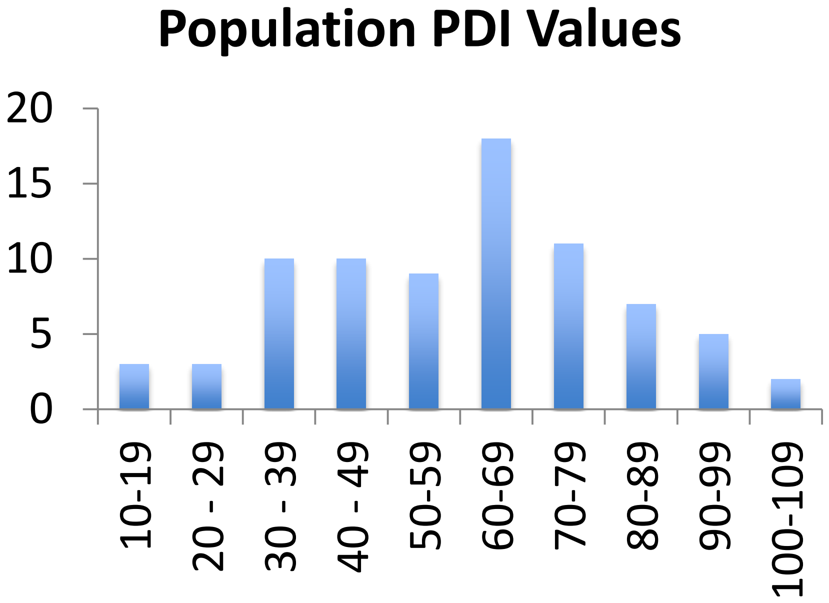
Sample Data

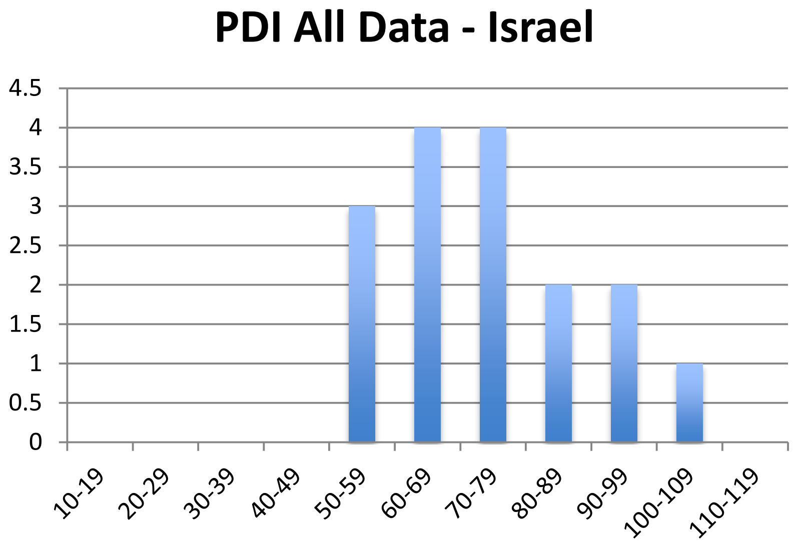


Results – PDI (All Data – II)

Control Data

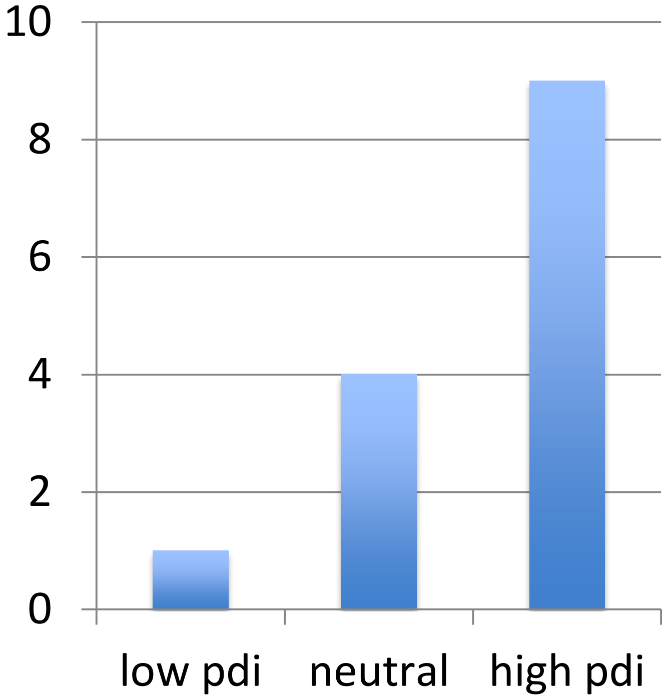
Sample Data



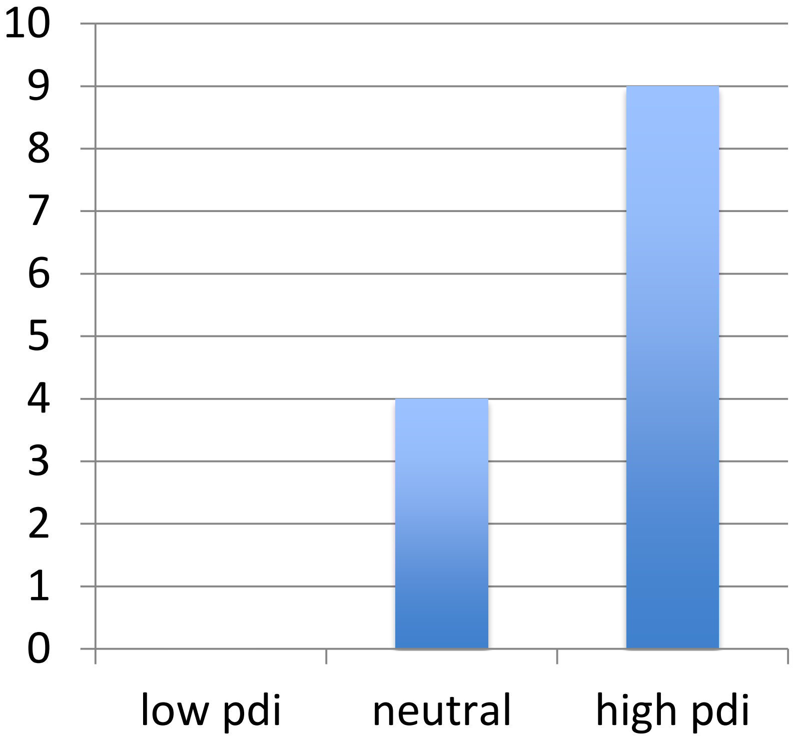


Results – PDI (Useable Data)

PDI With Israel

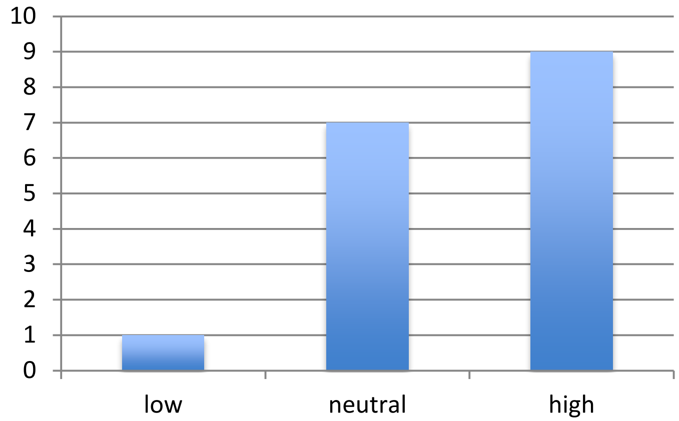


PDI Without Israel

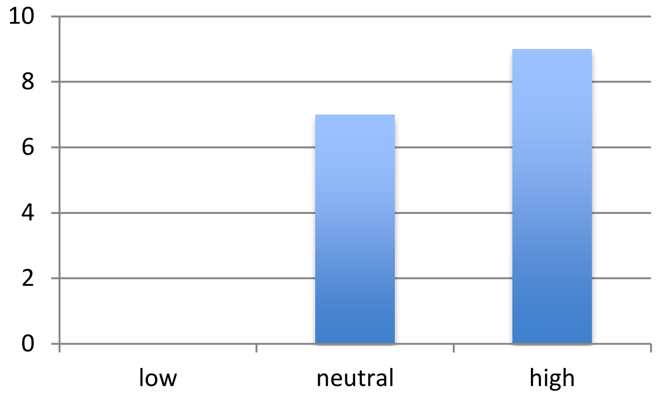


Results – All Data PDI

PDI With Israel

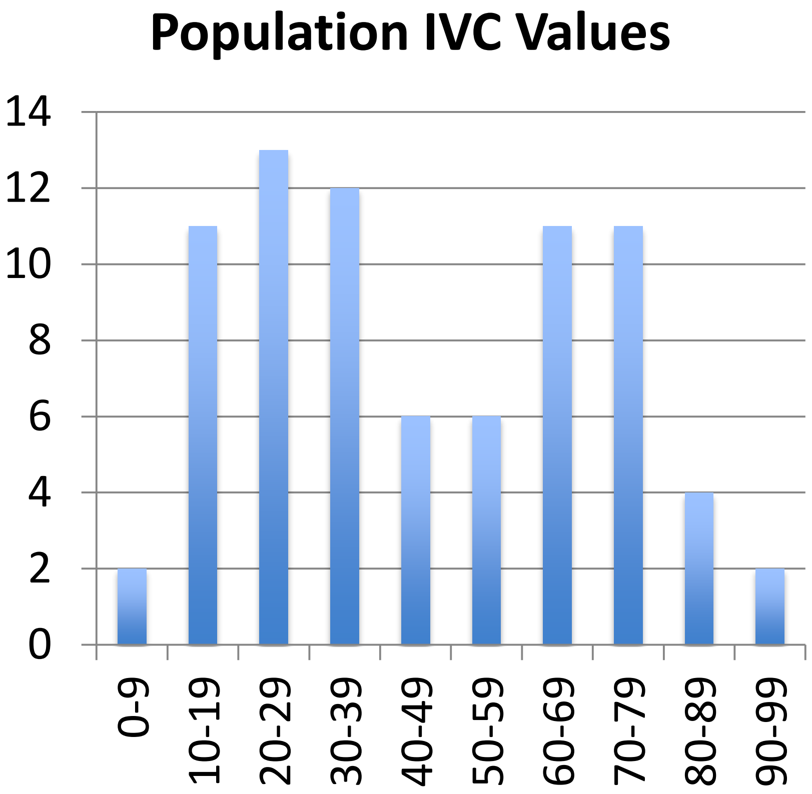


PDI Without Israel

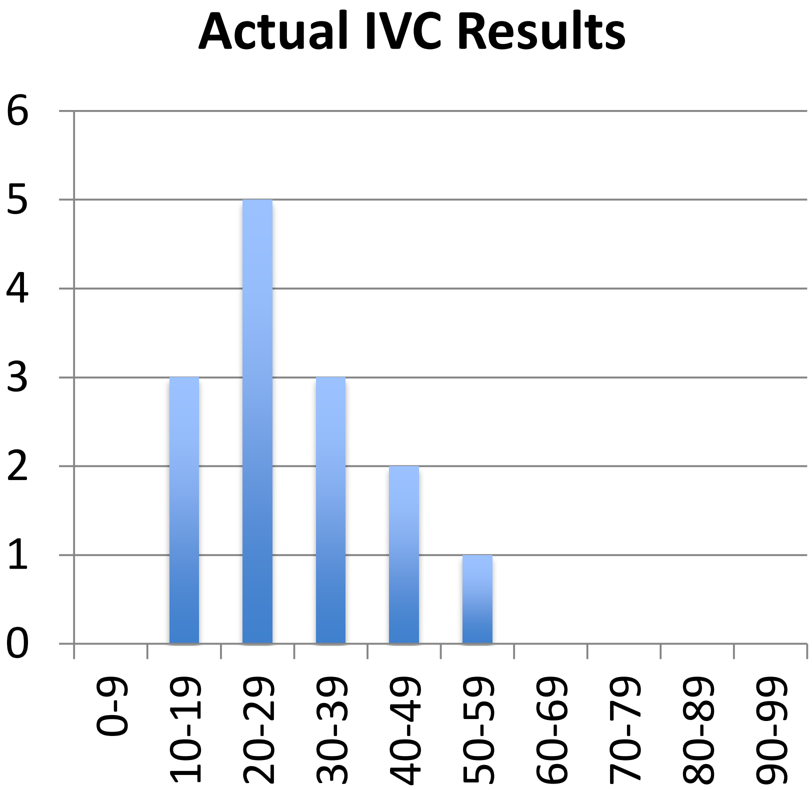


Results – IVC (Useable Data)

Control Data

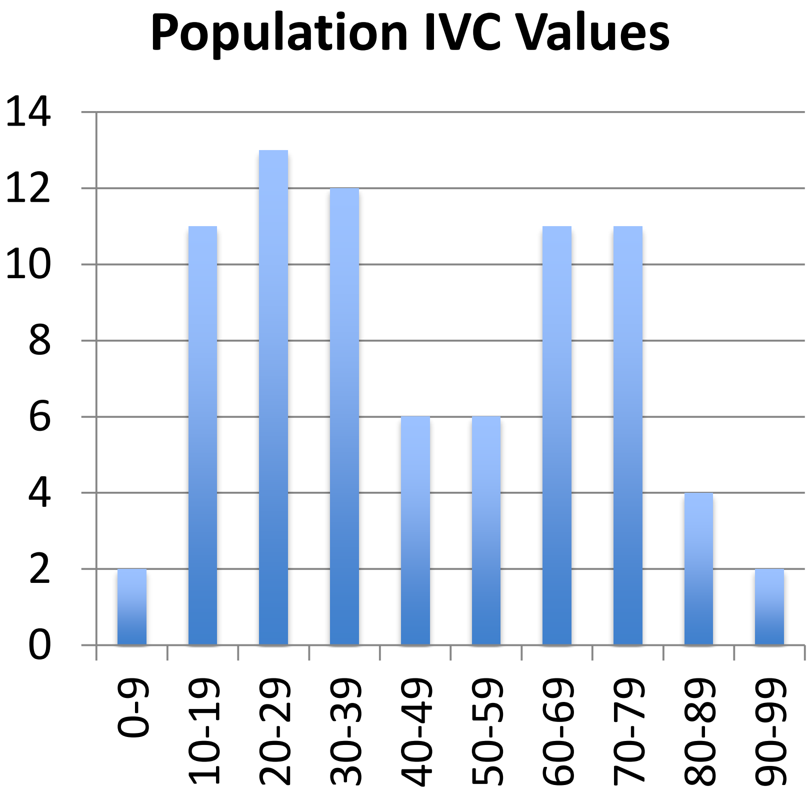


Sample Data

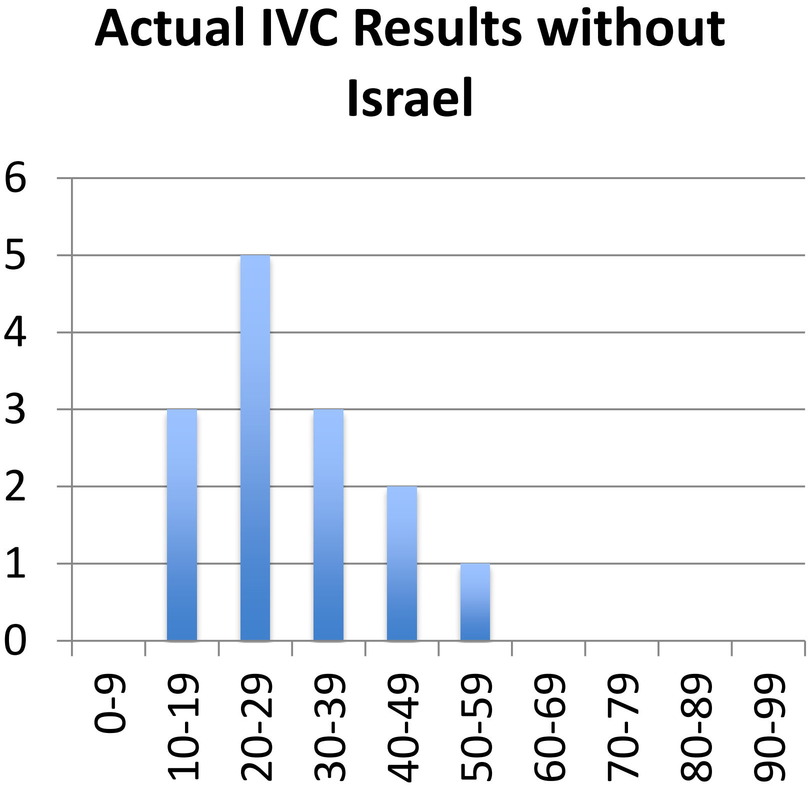


Results – IVC (Useable Data)

Control Data

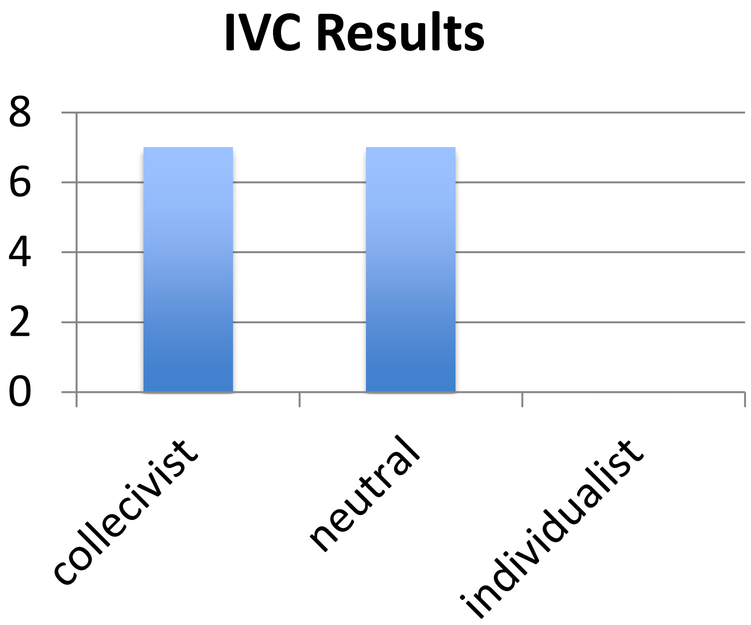


Sample Data

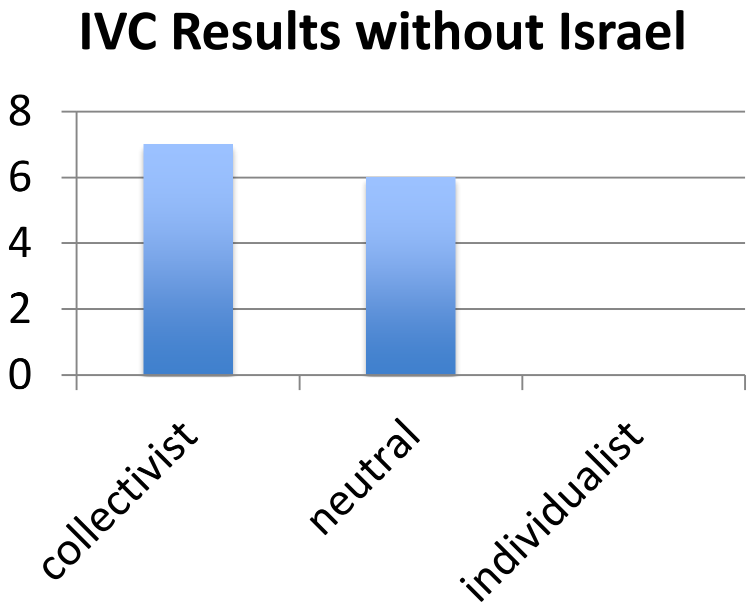


Results - IVC (Useable Data)

IVC With Israel



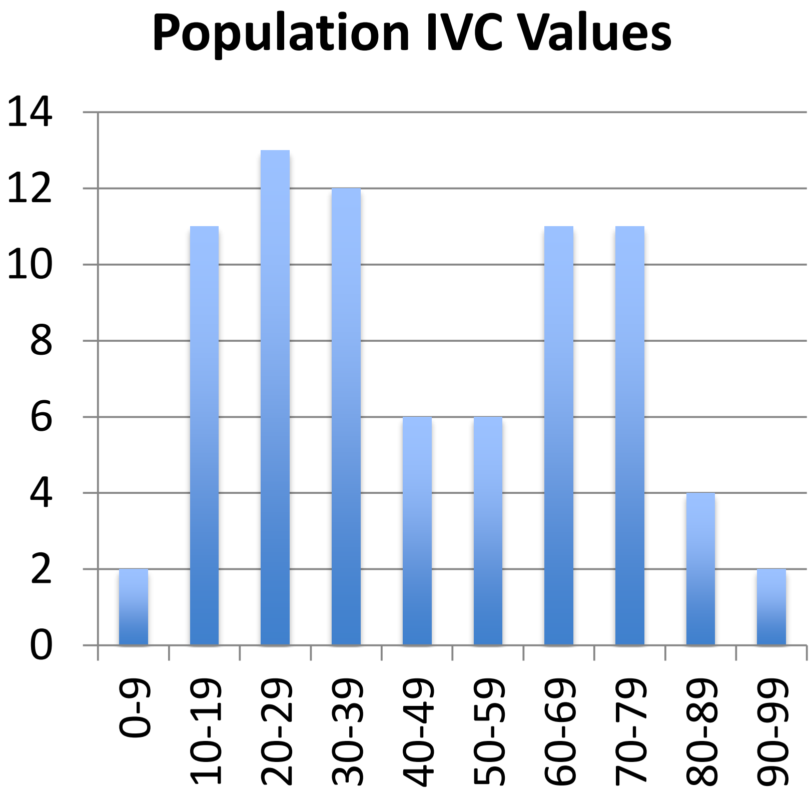
IVC Without Israel



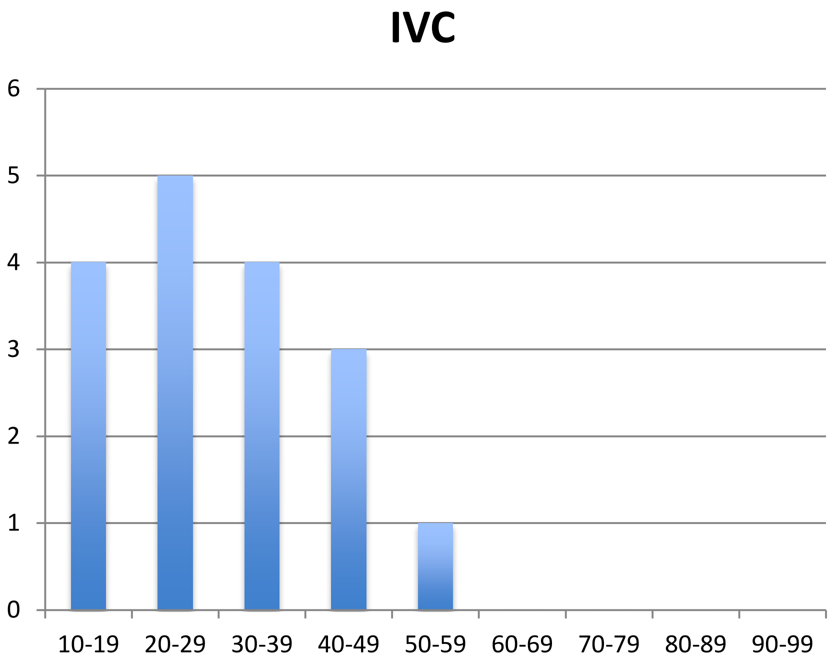
(c) Copyright 2013. All rights reserved.

Results IVC (All Data)

Control Group

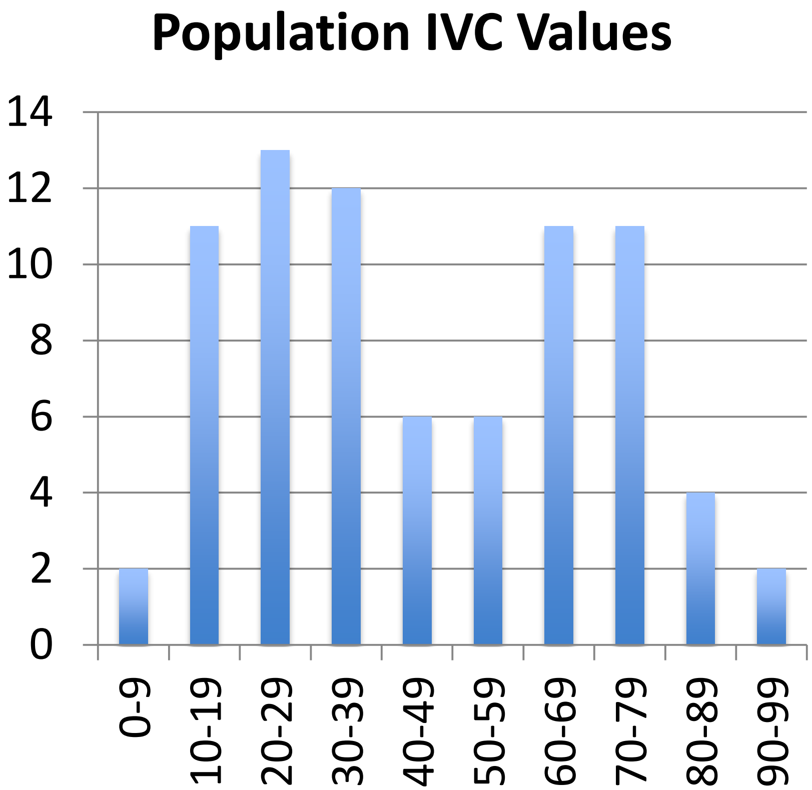


Actual Results IVC All Data

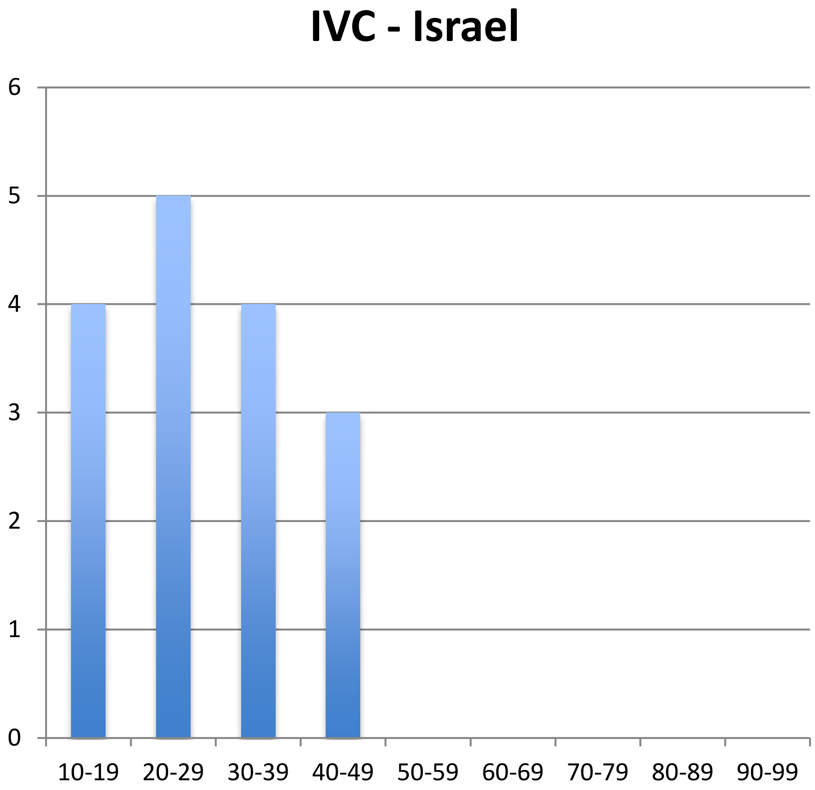


Results IVC (All Data - Il)

Control Group

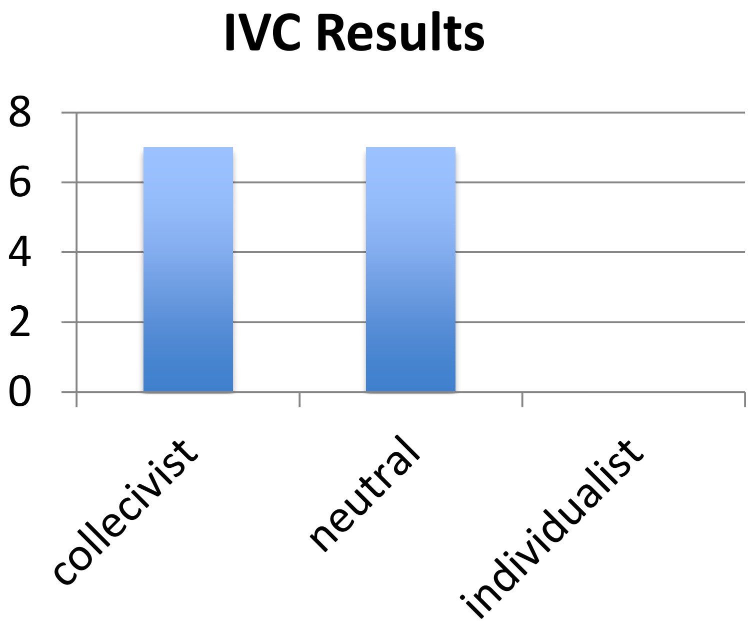


Actual Results IVC All Data - Il

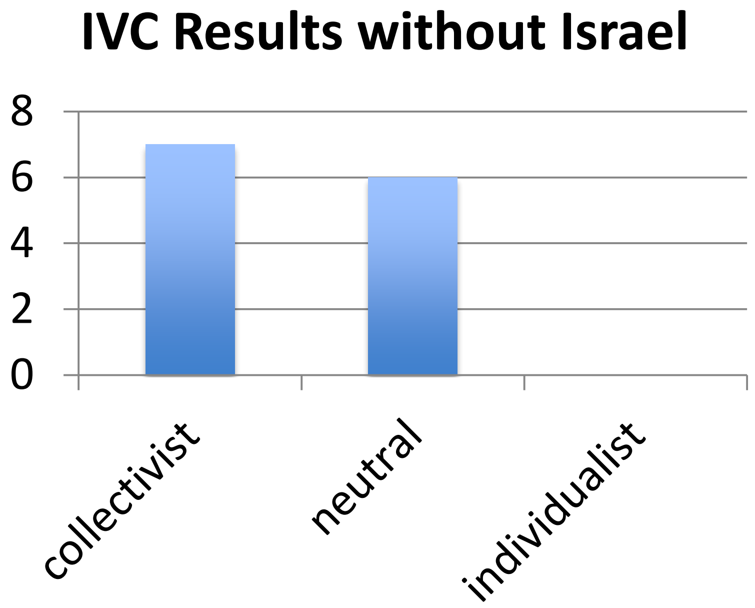


Results - IVC (All Data)

IVC With Israel

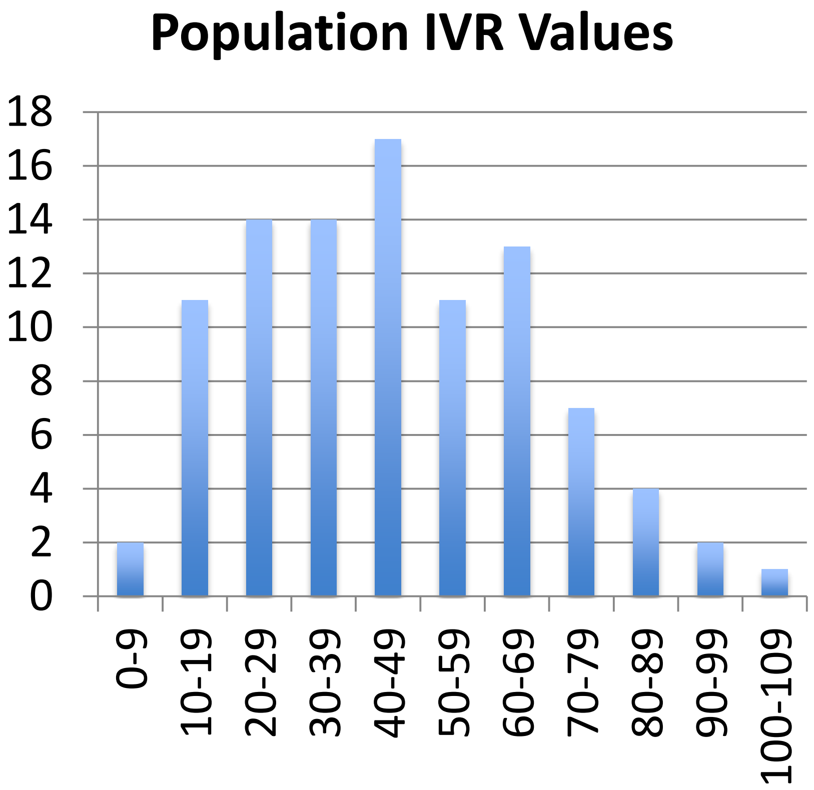


IVC Without Israel

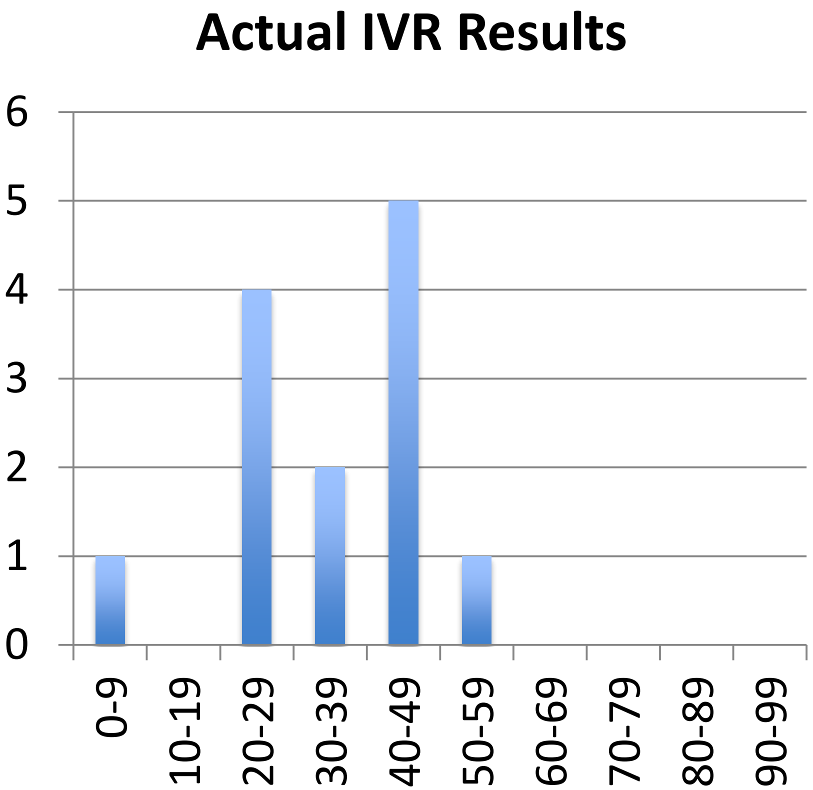


Results – IVR (Useable Data)

Control Data

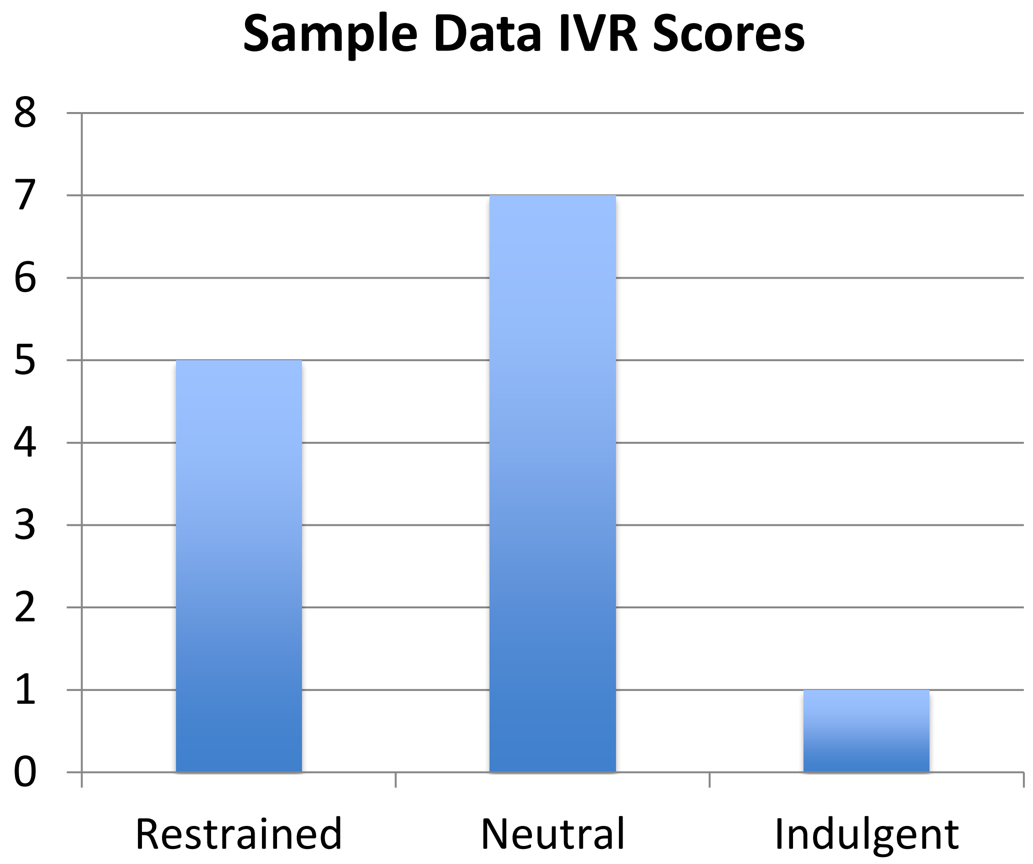


Sample Data



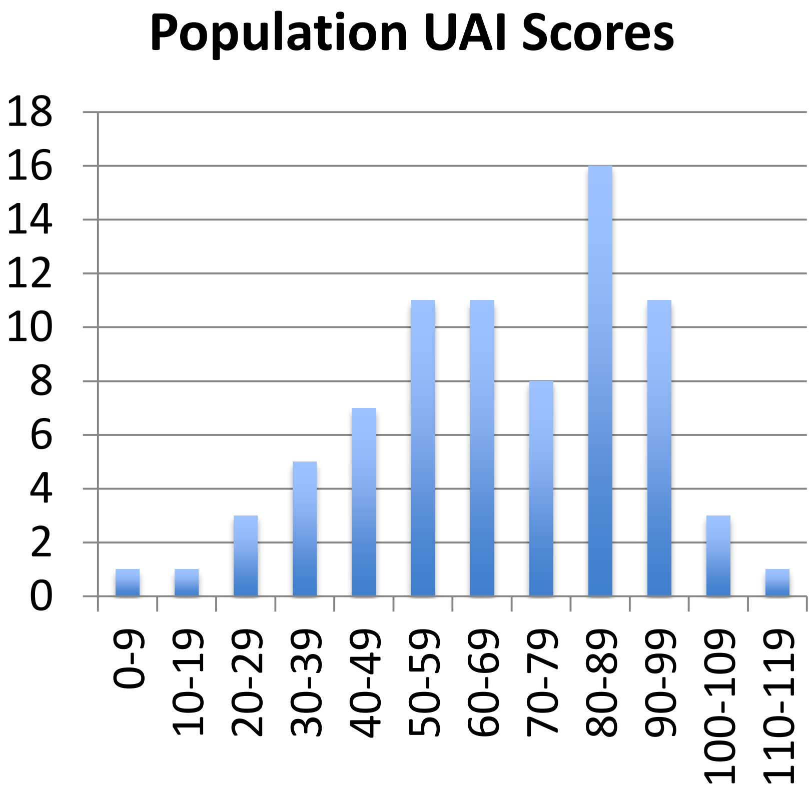
Results – IVR (Useable Data)

- Data for this dimension characteristics
  - Z Test Results z: 0.0307
  - Mann-Whitney Results: 0.0655

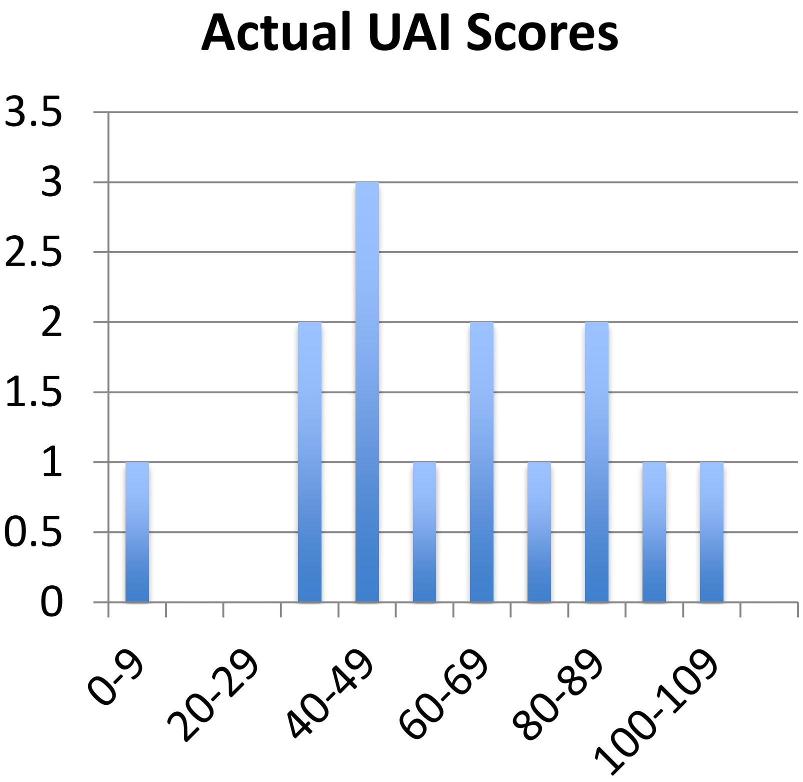


Results – UAI (Useable Data)

Control Data

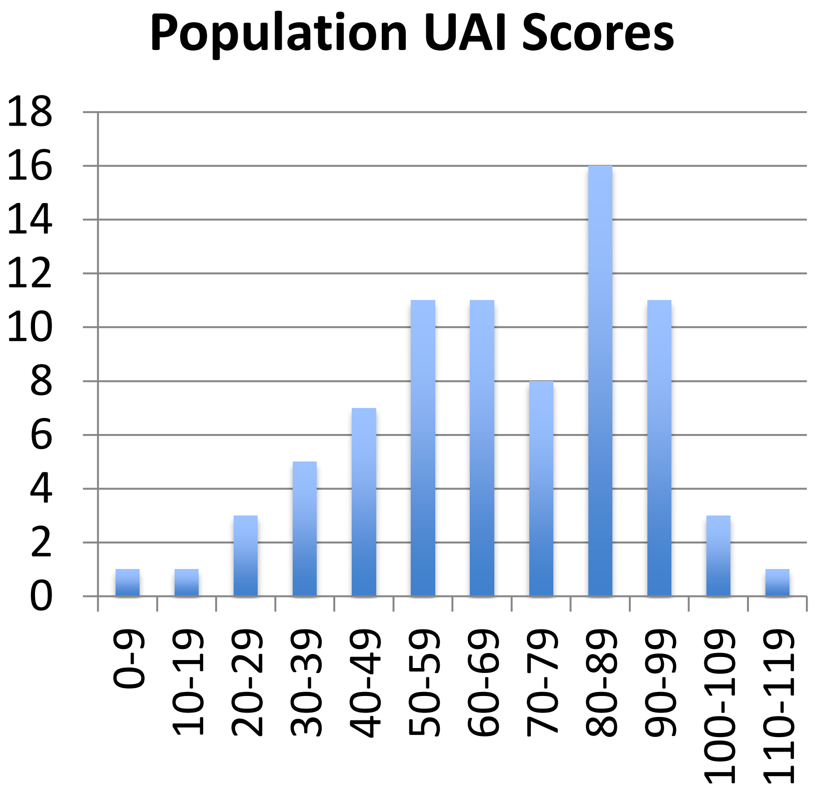


Sample Data

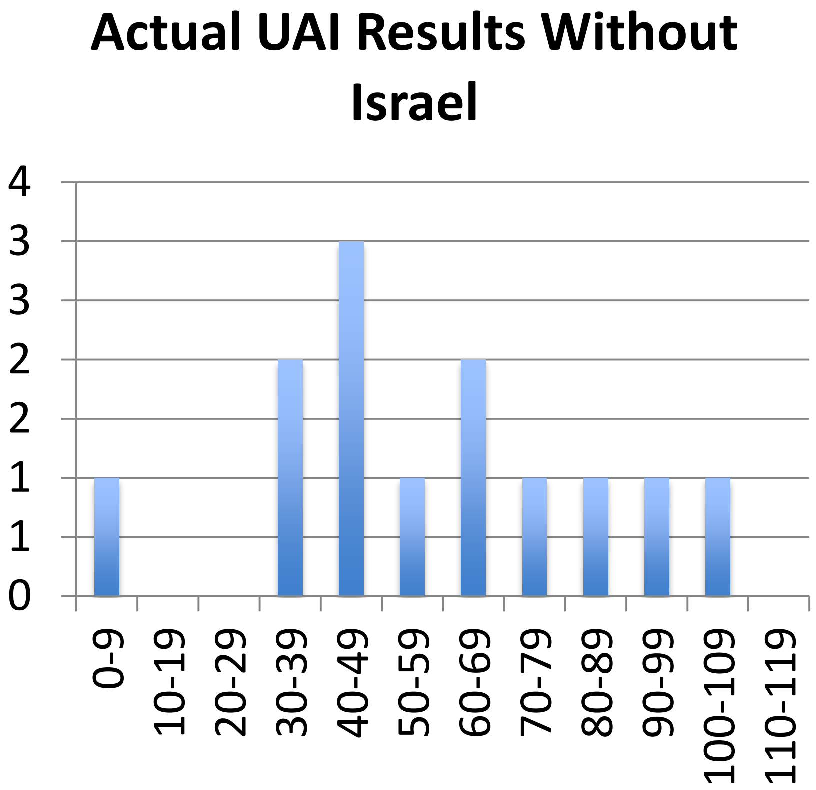


Results – UAI (Useable Data)

Control Data

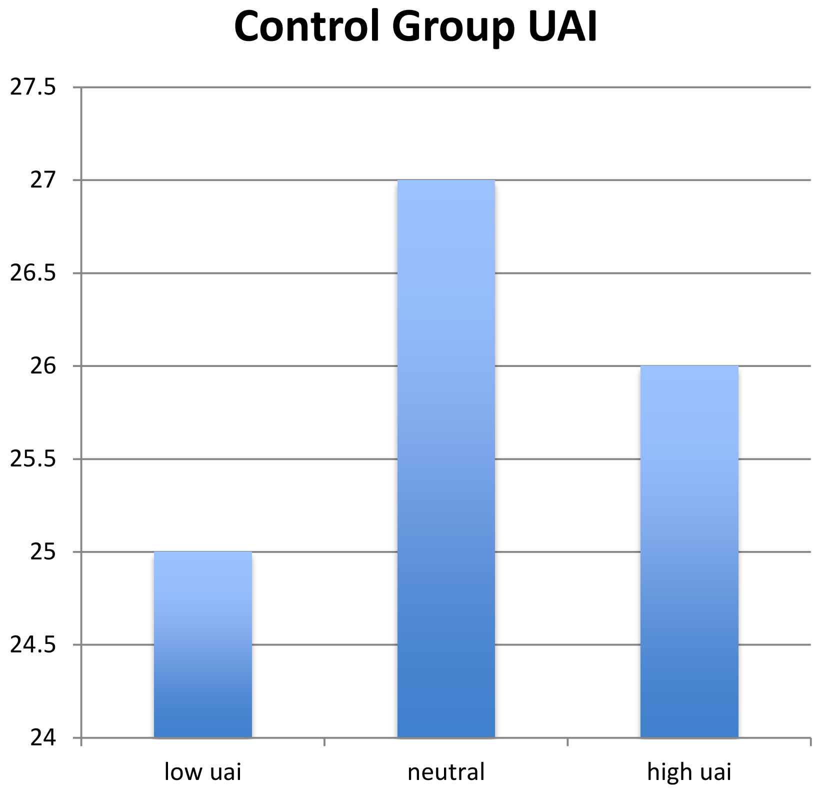


Sample Data

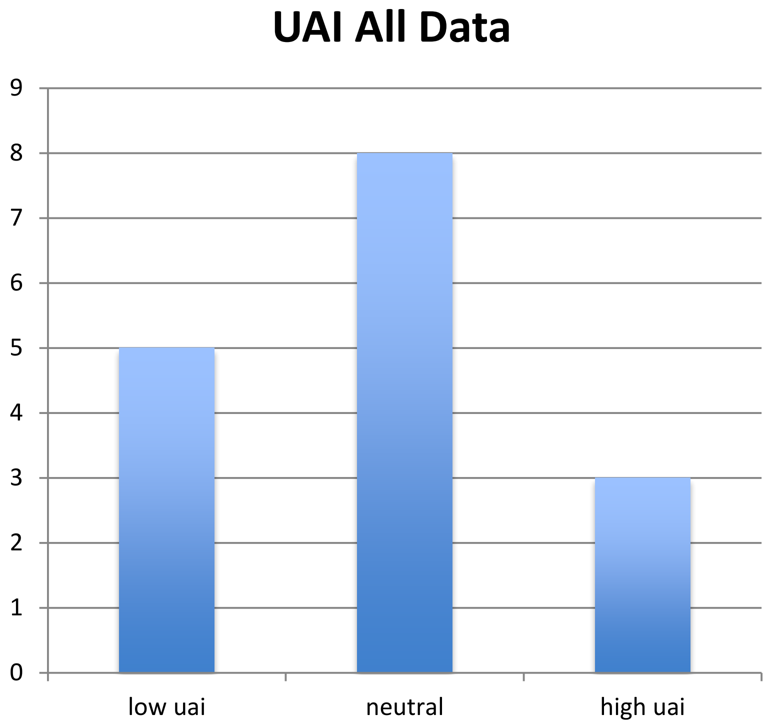


Results - UAI All Data

Control Data



Actual Results All Data



RESEARCH QUESTION #2

Results (2)

Control Group (2012) Values

- Africa East - 1 (77, 20, 46, 54, 9, 78)
- Brazil – 1 (67, 38, 49, 76, 44, 59)
- China – 3 (80, 20, 66, 30, 87, 24)
- Germany – 1 (35, 67, 66, 30, 87, 24)
- India – 2 (77, 48, 56, 40, 51, 26)
- Iran – 1 (58, 41, 43, 59, 14, 40)
- Japan – 1 (54, 46, 95, 92, 88, 42)
- Mexico -1 (81, 30, 69, 82, 24, 97)
- Russia – 1 (93, 39, 36, 95, 81, 20)
- UK – 1 (35, 89, 66, 35, 51, 69)
- US – 2 (40, 91, 62, 46, 26, 68)

Sample Group Values

- Canada FR – 1 (54, 73, 45, 60, n, n)
- Germany – 1 (35, 67, 66, 30, 87, 24)
- Greece – 1 (60, 35, 57, 112, 45, 50)
- Philippines – 1 (94, 32, 64,44, 27, 42)
- Russia – 1 (93, 39, 36, 95, 81, 20)
- UK – 4 (35, 89, 66, 35, 51, 69)
- US – 6 (40, 91, 62, 46, 26, 68)

Results (2)

Results of Research Question Two Using 2012 Control Group

Hypothesis #	Test	Tool	U=	Z=	p-value	Accept/Reject
(PDI) $H2_{0,}$ $H2_1$	μ >= 59	Mann-Whitney	162	**-2.03**	**0.0212**	**Reject**
(IVC) $H2_{0,}$ $H2_2$	μ <= 45	Mann-Whitney	51	**2.53**	**0.0057**	**Reject**
(M/F) $H2_{0,}$ $H2_3$	μ <= 50	Mann-Whitney	114	-0.04	0.484	Accept
(UAI) $H2_{0,}$ $H2_4$	μ >= 68	Mann-Whitney	113	0	0.5	Accept
(STO)$H2_0$, $H2_5$	μ >= 45	Mann-Whitney	125	0.85	0.1977	Accept
(IVR) $H2_{0,}$$H2_6$	μ <= 45	Mann-Whitney	69	1.55	0.0606	Accept

Results (2)

Control Group (2004) Values

- Brazil – 1 (67, 38, 49, 76, 44, 59)
- China – 3 (80, 20, 66, 30, 87, 24)
- Germany – 1 (35, 67, 66, 30, 87, 24)
- France – 1 (68, 71, 43, 86, 63, 48)
- India – 1 (77, 48, 56, 40, 51, 26)
- Iran – 1 (58, 41, 43, 59, 14, 40)
- Japan – 2 (54, 46, 95, 92, 88, 42)
- Mexico -1 (81, 30, 69, 82, 24, 97)
- Russia – 1 (93, 39, 36, 95, 81, 20)
- US – 2 (40, 91, 62, 46, 26, 68)

Sample Group Values

- Canada FR – 1 (54, 73, 45, 60, n, n)
- Germany – 1 (35, 67, 66, 30, 87, 24)
- Greece – 1 (60, 35, 57, 112, 45, 50)
- Philippines – 1 (94, 32, 64,44, 27, 42)
- UK – 2 (35, 89, 66, 35, 51, 69)
- US – 6 (40, 91, 62, 46, 26, 68)

Results (2)

Results of Research Question Two Control Group 2004 Data Smoothing

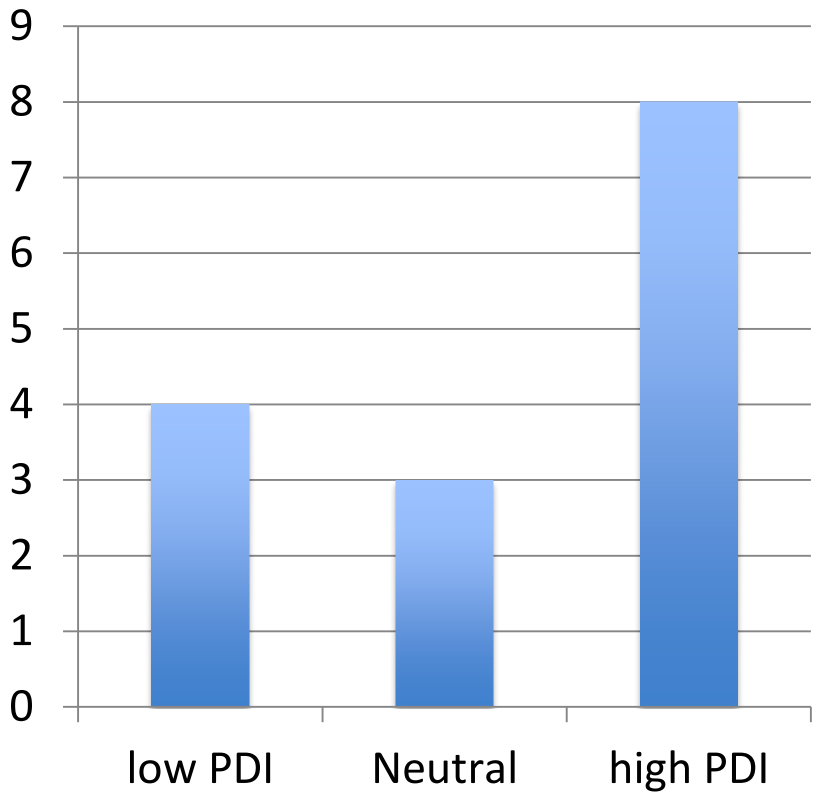
Hypothesis #	Test	Tool	U=	Z=	p-value	Accept/Reject
(PDI) $H2_0$, $H2_1$	μ >= 59	Mann-Whitney	109.5	**-2.14**	**0.0162**	**Reject**
(IVC) $H2_{0,}$ $H2_2$	μ <= 45	Mann-Whitney	35.5	**2.19**	**0.0143**	**Reject**
(M/F) $H2_{0,}$ $H2_3$	μ <= 50	Mann-Whitney	78	-0.32	0.3745	Accept
(UAI) $H2_{0,}$ $H2_4$	μ >= 68	Mann-Whitney	80.5	-0.46	0.3228	Accept
(STO) $H2_{0,,}$ $H2_5$	μ >= 45	Mann-Whitney	107.5	**2.52**	**0.0059**	**Reject**
(IVR) $H2_{0,}$ $H2_6$	μ <= 45	Mann-Whitney	20.5	**2.77**	**0.0028**	**Reject**

Results (2)

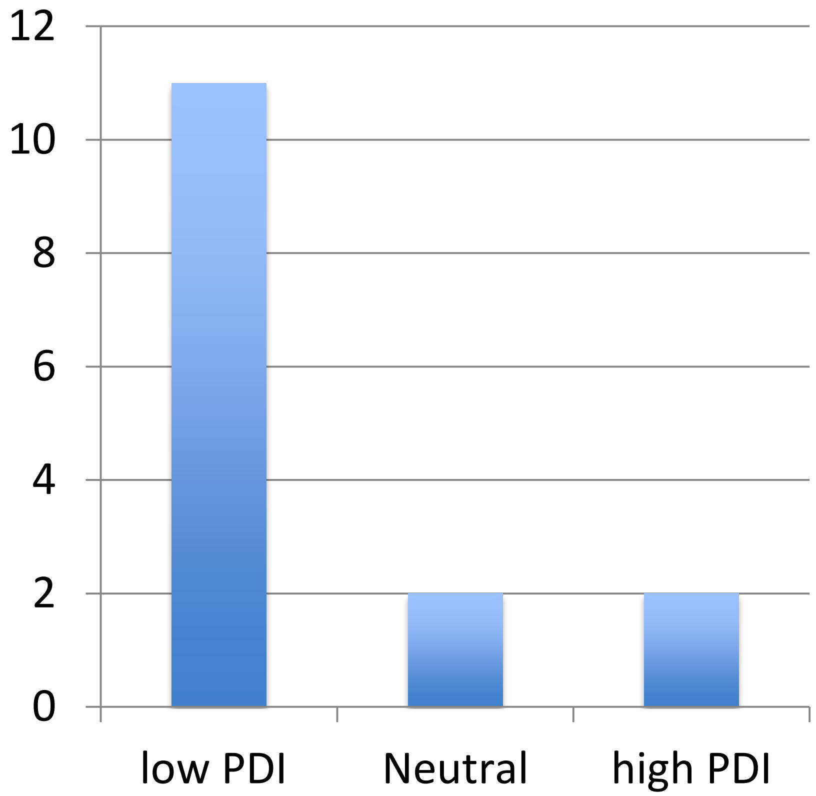
PDI	IVC	M/F	UAI	LTOvSTO	IVR
1	1	0	0	0 (1)	0 (1)

Note. 0 indicates the null hypothesis was accepted for the dimensional question and 1 indicates that the null hypothesis was rejected.

Results - PDI (2)

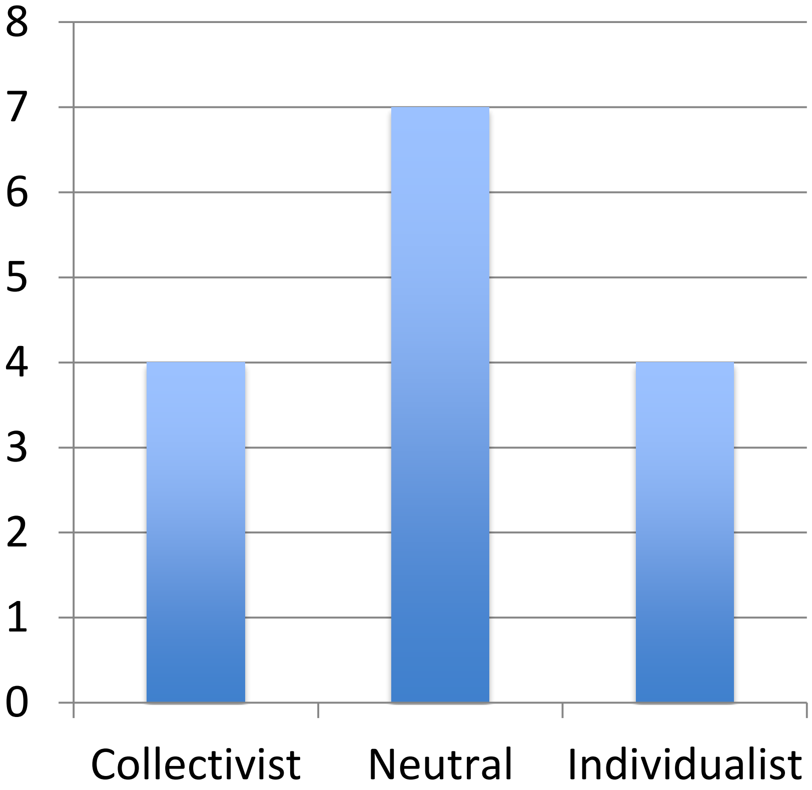


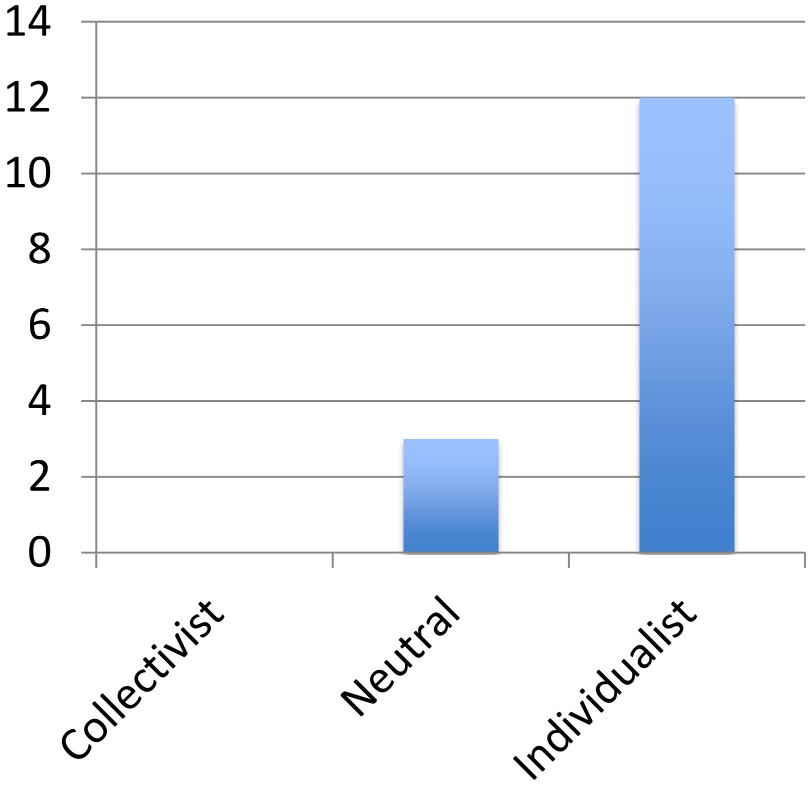
Control Data PDI - 2012



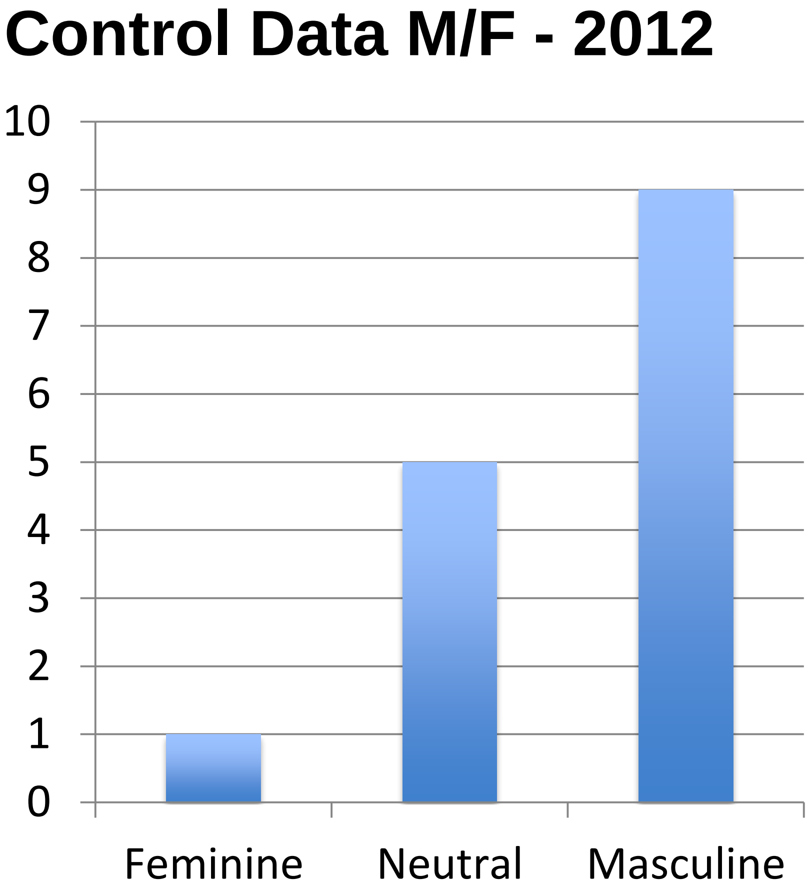
Sample Data PDI - 2012

Results – IVC (2)

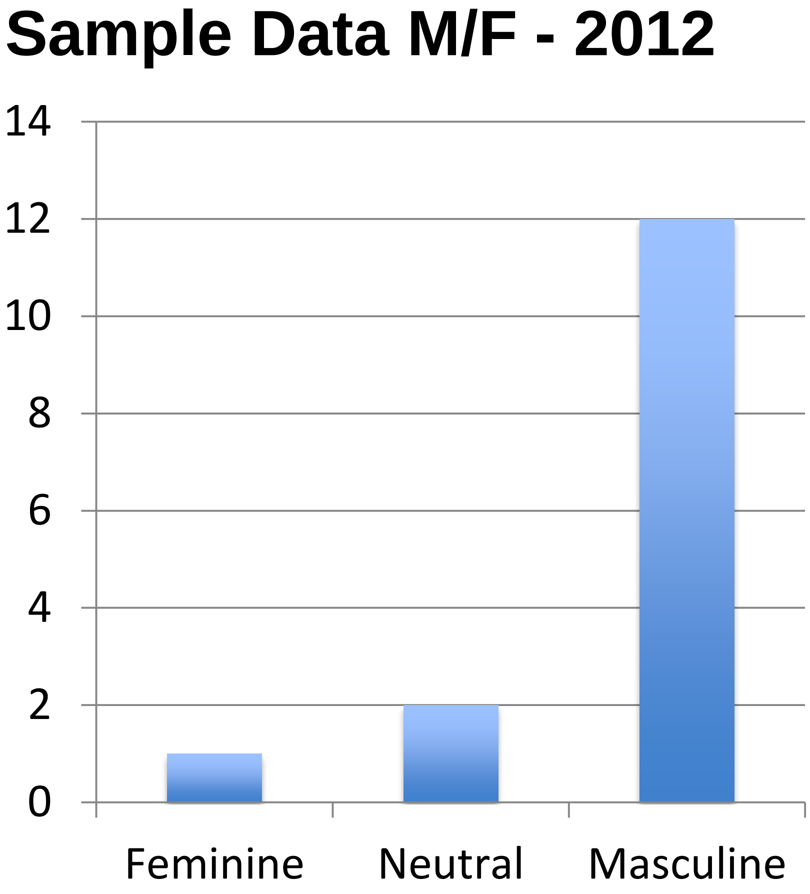

Control Data IVC - 2012


Sample Data IVC -2012

Results – M/F (2)



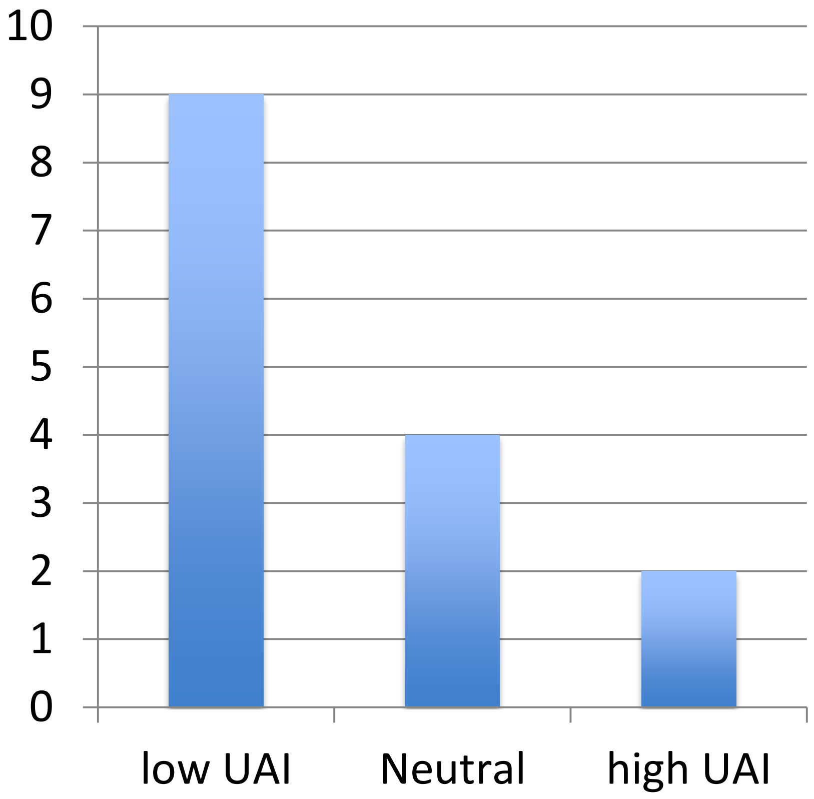
Control Data M/F - 2012
10
9
8
7
6
5
4
3
2
1
0
Feminine
Neutral
Masculine



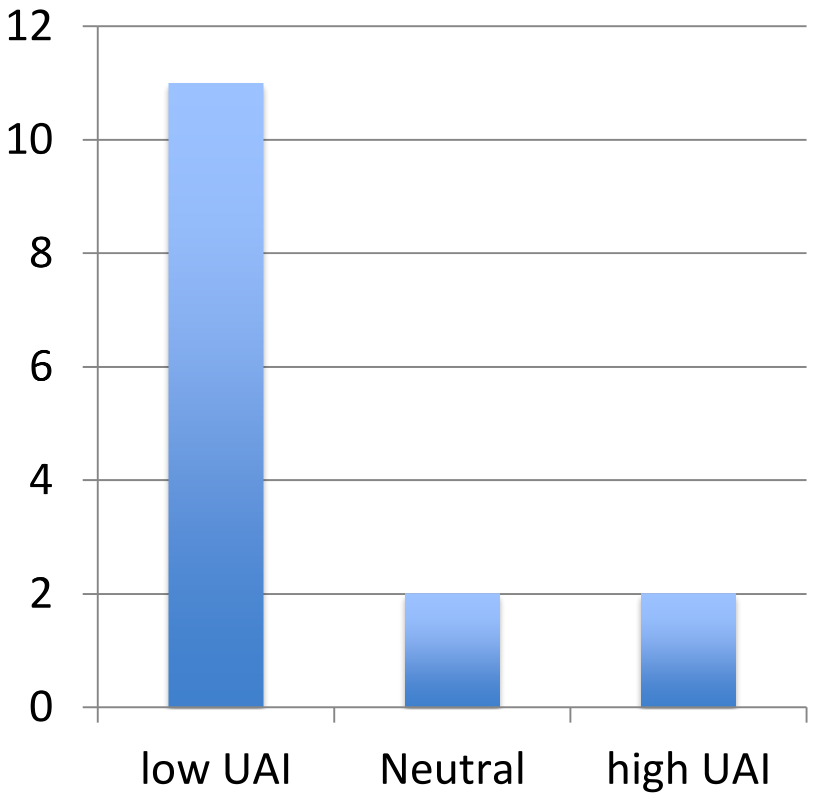
Sample Data M/F - 2012
14
12
10
8
6
4
2
0
Feminine
Neutral
Masculine

Results – UAI (2)

Control Data UAI - 2012

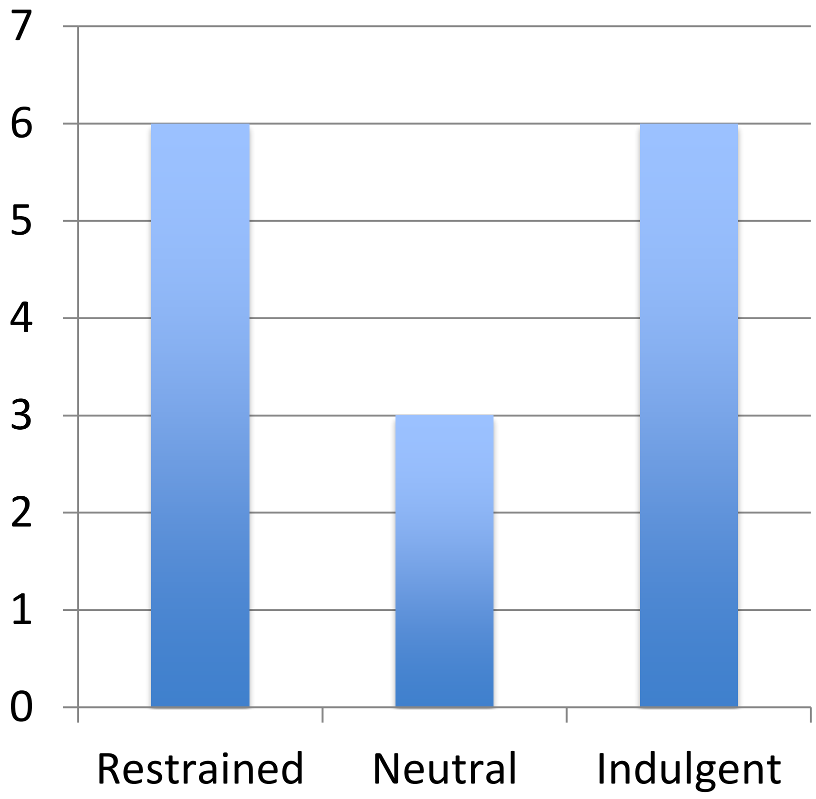


Sample Data UAI - 2012

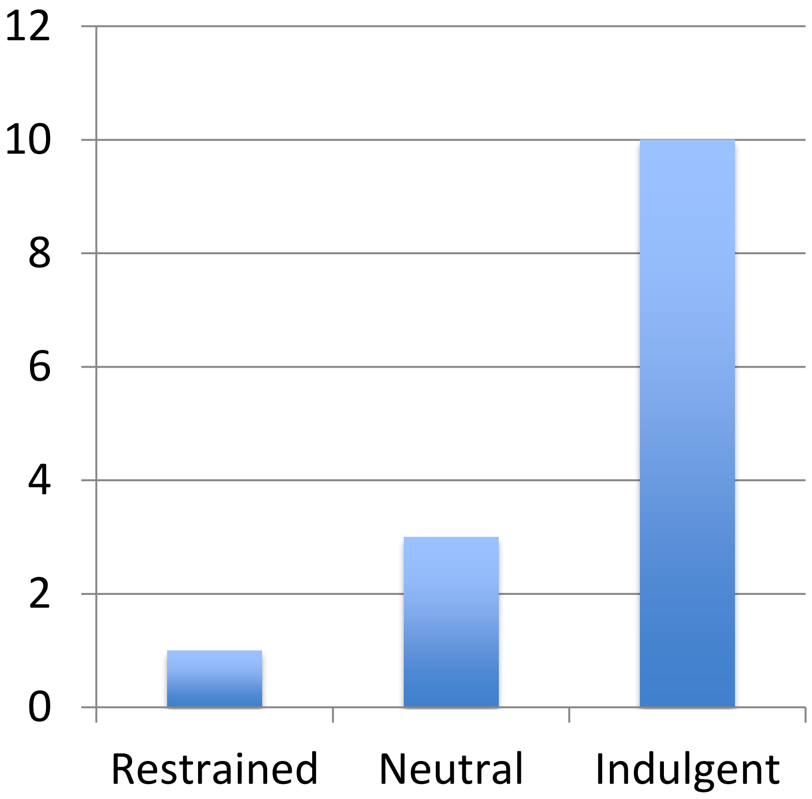


Results – IVR (2)

Control Data IVR - 2012



Sample Data IVR - 2012



Conclusions

- Results
  - Statistically significant relationship between high PDI and low IVC dimensions and nationalistic, patriotic themed website attacks.
  - Statistically significant relationship between low PDI and high IVC dimensions and “lone wolf” attacking behaviors.
  - Notable observations in IVR and UAI.
- Next Steps
  - Expand using larger datasets.
    - Correlational studies pdi data from zone-h.org
  - Focus questions for other dimensions examining for cultural traces in other activities such as software coding, malware behaviors, attack strategies or TTPs…
    - UAI malware
    - UAI coding errors

Conclusion

- There appears to be relationship between culture and certain CNA behaviors.
  - Means testing using Mann-Whitney verified 2 of 6 dimensions.
  - An even more interesting finding was the lack of activity in certain ends of specific dimensions.
    - Low power distance
    - Individualism
    - High uncertainty avoidance
    - Short term orientation
    - Indulgence

Thank you!

Dr. Char Sample
csample@cert.org or charsample50@gmail.com
CERT/NetSA 2013

Cultural Research

- Dr. Dominck Guss (Guess, 2004)
  - Funded in part by NSF to examine cognitive processing.
  - Discussed basic assumptions then asked (2011)
    - “Does culture influence how students learn”?
    - If so “does this leave traces”?
  - Pointed to Dr. Hofstede’s work and sent some papers my way.
    - Dr. Dominik Guss & Dietrich Dorner (2010) observed that ***culture influences problem perception, strategy development and the decision choices***.
    - This mental software is subconsciously used during problem solving situations (Hofstede 2001, Guss, & Dorner 2010).

Cultural Research

- Guss’s (continued):
  - Findings (continued)
    - Guss and Wiley (2007) noticed that novel problems resulted in the ***problem solvers relying on culturally developed and learned strategies*** to solve the problem.
    - “***Strategies were even stronger predictors of performance*** than the control variables computer experience and intelligence” (2011).
    - Culture influences: **perception, categorization, and reasoning** (2011).
- Other’s
  - Berry (2004) and Strohschneider (2001) also observed that development of problem solving strategies vary by culture.
  - Bornstein, Kugler, & Ziegelmeyer (2003) observed cultural differences with decision making in game playing experiments.

Parameters of Culture

- Parameters
  - Does not reflect differences between individuals.
  - Statements about cultures are general and relative.
  - The appeal of culture lies in the fact that the people's thought processes subconsciously reflect their cultural background.
    - While not great for individual hacker attribution it has cyberwar implications: defensive and offensive.
    - Markers, if they exist, ***should*** reveal themselves, even with re-used attacks.

Research Plan(2)

- Why inferential quasi-experiment vs correlation or causal research plans.
  - The type of data available largely determines the method.
    - Unable to meet academic criteria for data with any accuracy.
  - Choosing quantitative research limited options.
    - Quantitative chosen controversy that it can generate was chosen due in part to the nature of this study.

Conclusion

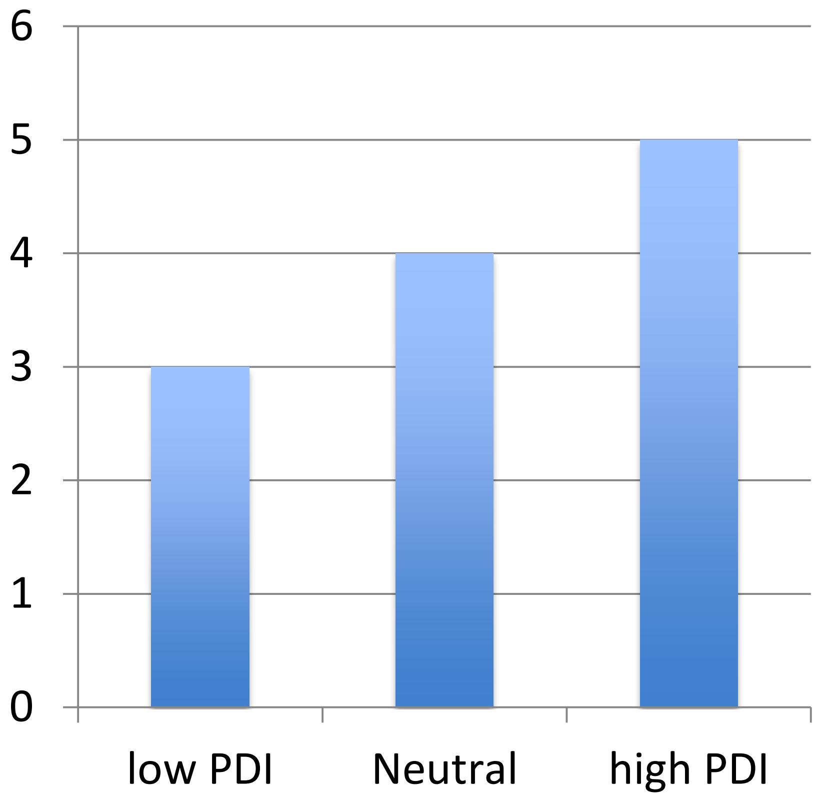
- This approach relies on unconscious thought patterns of attackers that have been institutionalized through national education systems.
- This researcher hopes to provide evidence that culture does play a role in CNA choices and behaviors.
- The literature reviewed supports the hypothesis, data is currently being collected.
- There is much more work to be done, if this hypothesis proves correct.
- The current study, while promising is limited in scope, more information is needed on each dimension and associating attacks within each dimension.

In Other Words

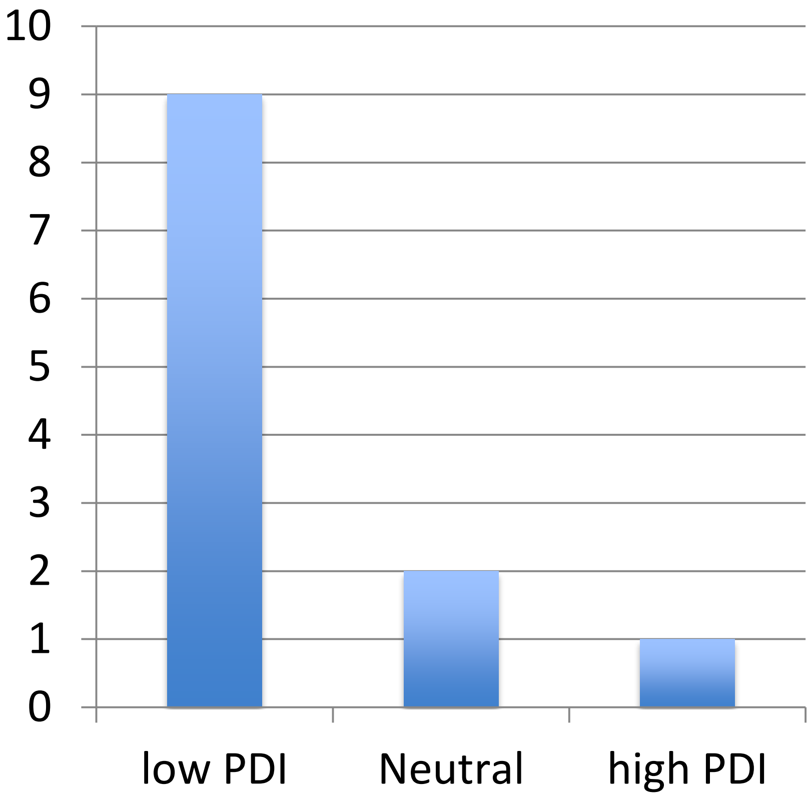
- System 360
- Google

Results - PDI (2)

Control Data PDI - 2004

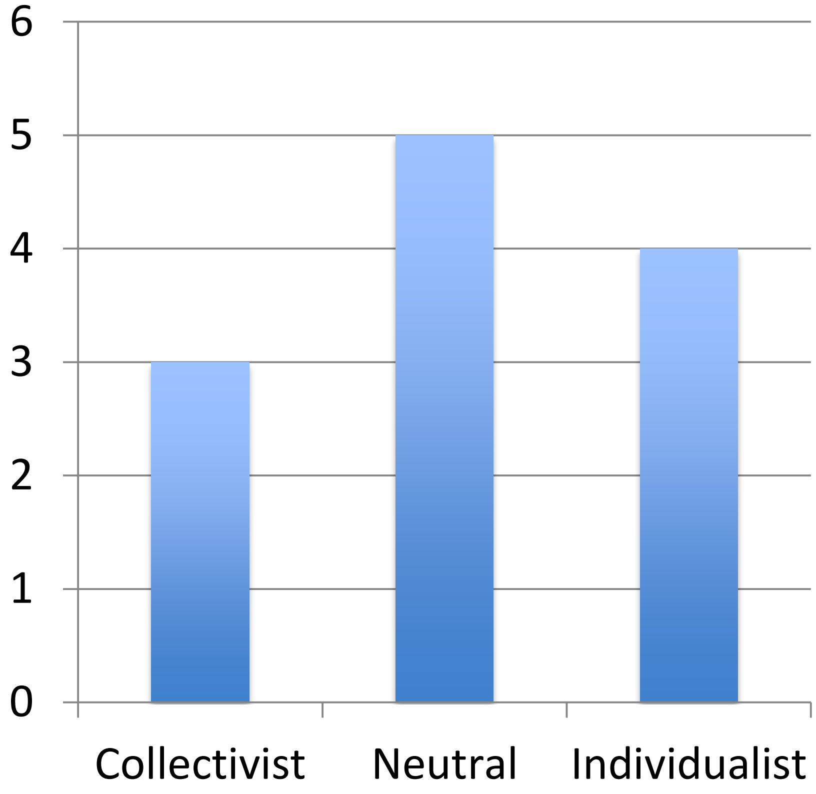


Sample Data PDI - 2004

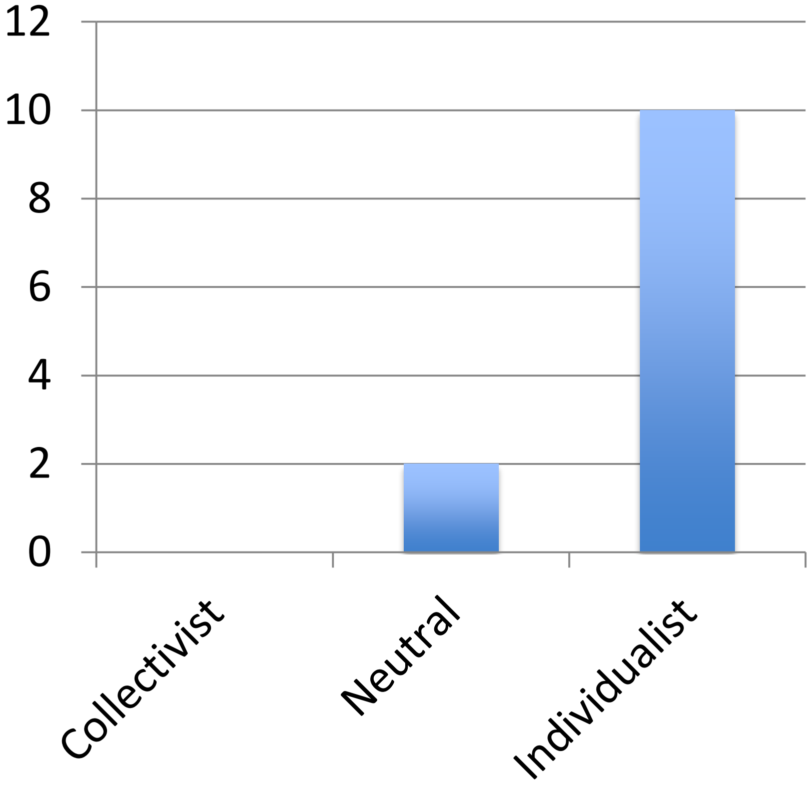


Results – IVC (2)

Control Data IVC - 2004

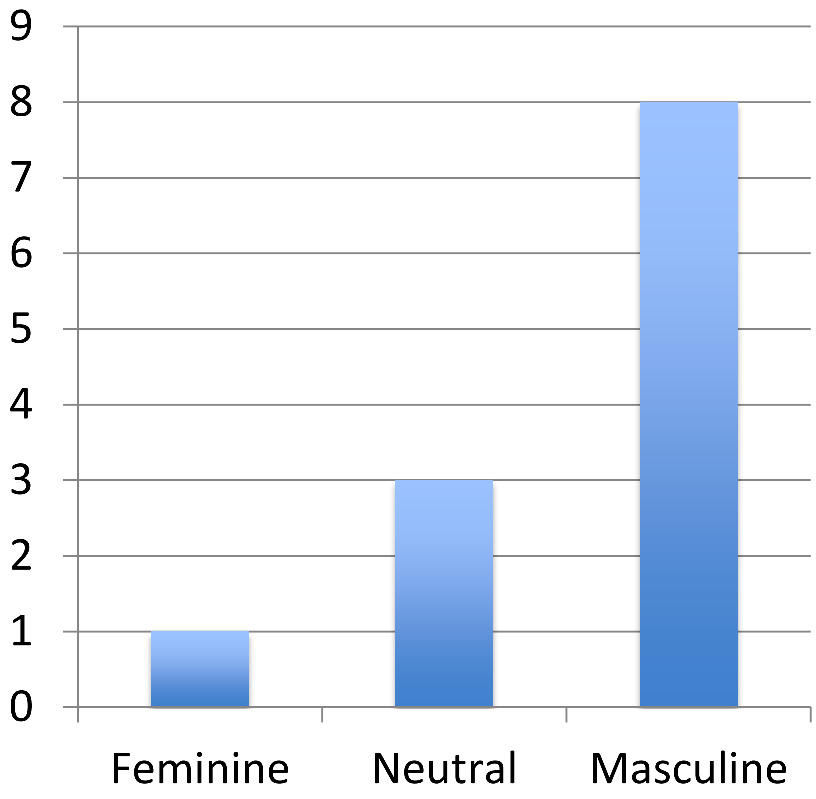


Sample Data IVC -2004

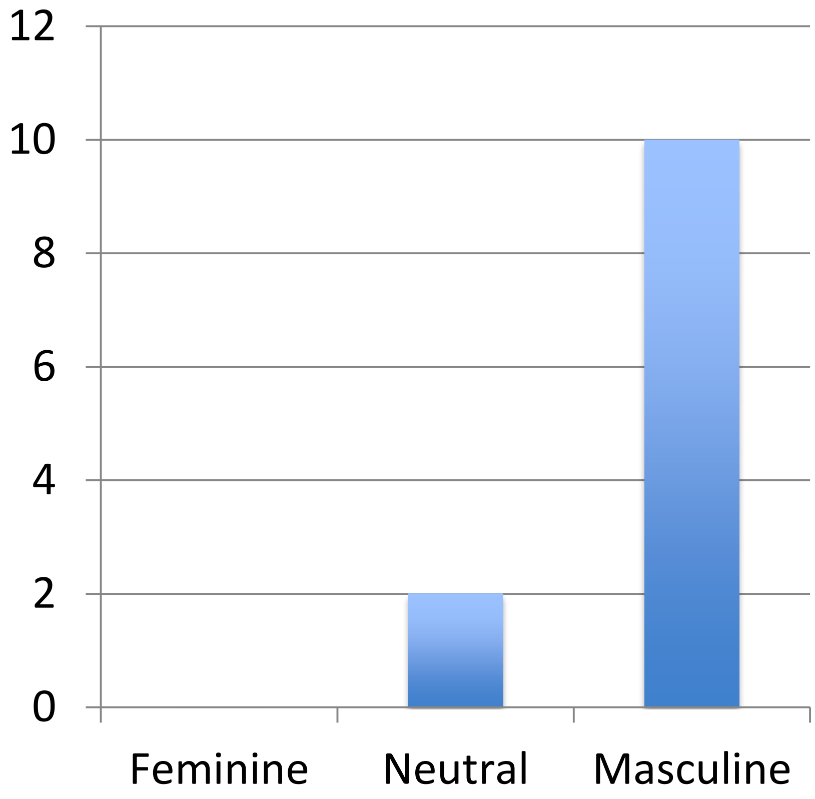


Results – M/F (2)

Control Data M/F - 2004

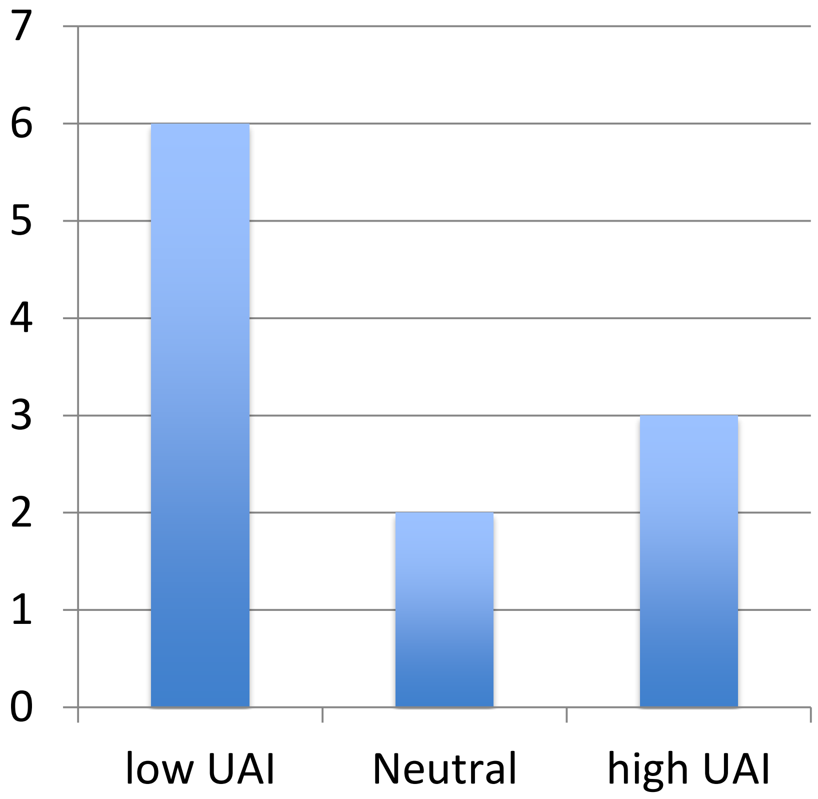


Sample Data M/F - 2004

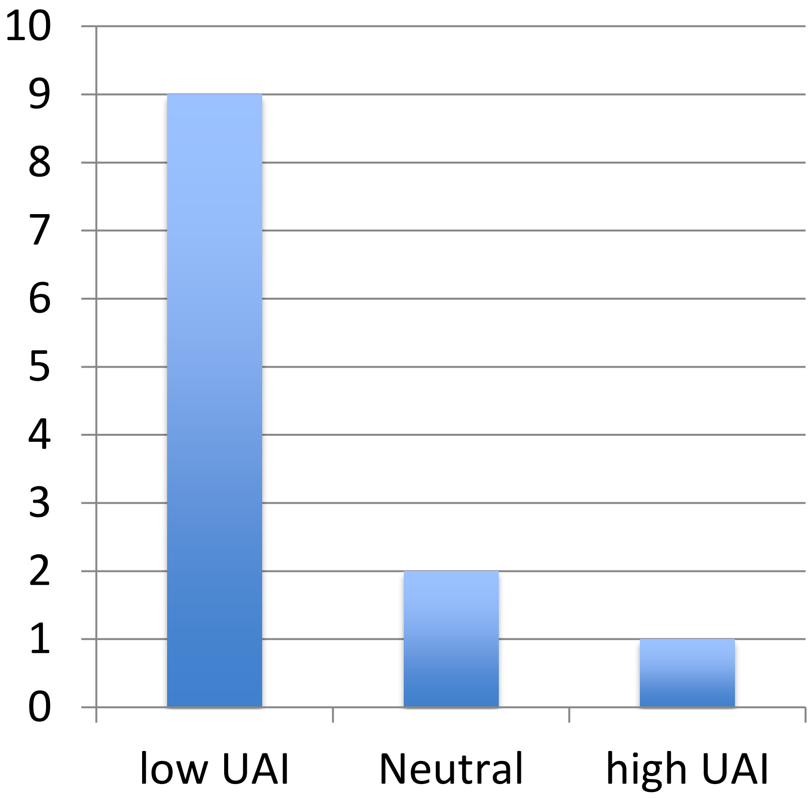


Results – UAI (2)

Control Data UAI - 2004

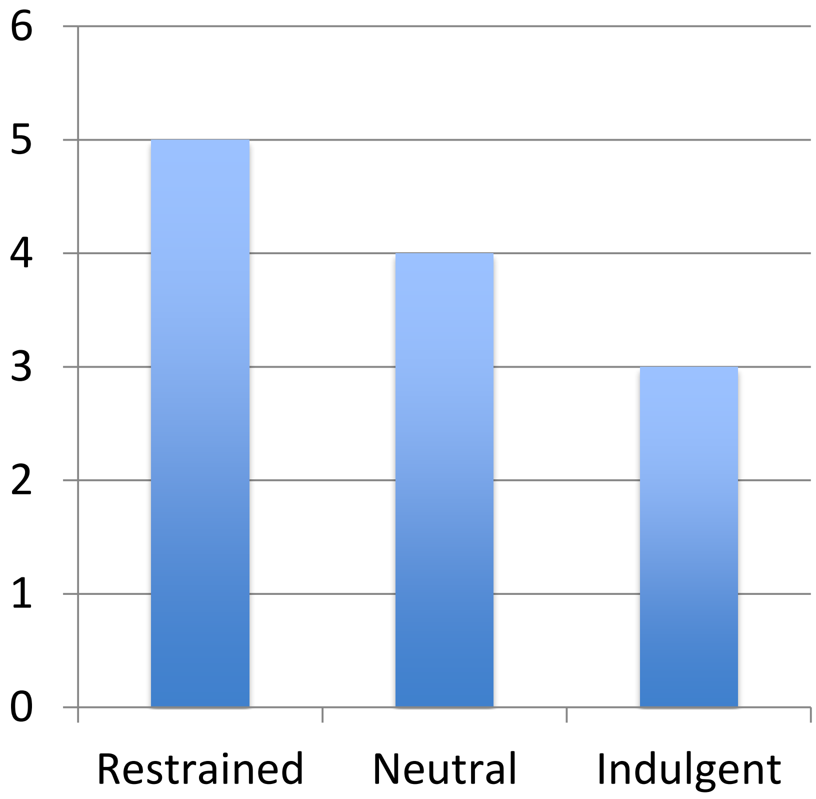


Sample Data UAI - 2004

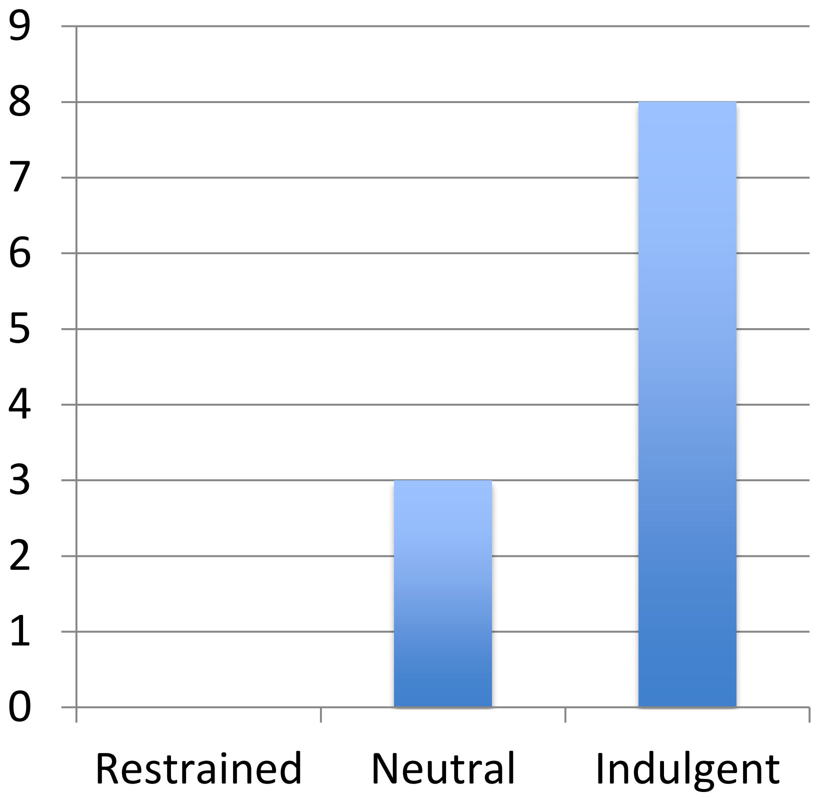


Results – IVR (2)

Control Data IVR - 2004



Sample Data IVR - 2004


Restrained
Neutral
Indulgent