



National Culture in Cyber Security


Dr. Char Sample, Dr. Jennifer Cowley
& Steve Hutchinson
CASE Workshop NSU
June 7-8, 2017

Culture

“Culture, like an onion, consists of layers that can be peeled off.”

(Trompenaars 2003 p25)

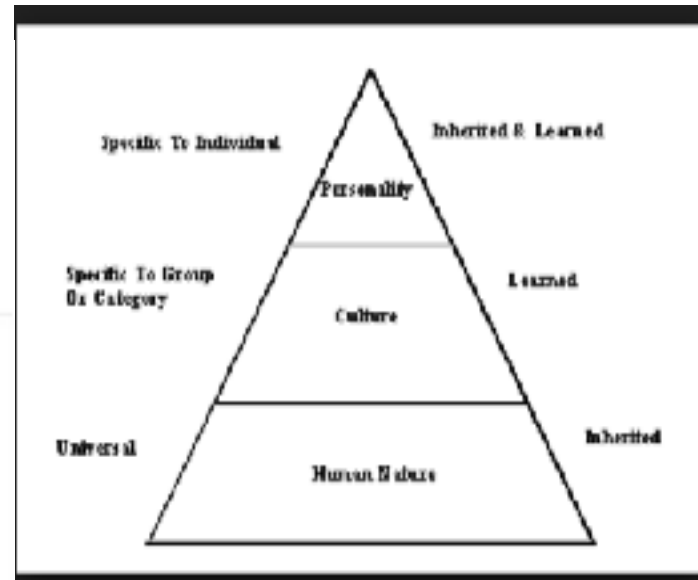
Visual Cultural Differences



Language
Housing
Food
Clothes

Key Beliefs
Not so visible but has an effect on determining behaviour at a more superficial level


Norms and Values
greetings
bow, shake hands




East vs West
Do They Think & Perceive Differently?

Which TWO go together?


- Chicken and Grass?
- Cow and Chicken?
- Grass and Cow?



COW



GRASS



CHICKEN

Culture

What is culture?

- “Mental software”
- Shared values
- Shared beliefs
- Shared problem solving

Why does culture matter?

- Sets norms
- Shapes perception
- Predicts responses

Hofstede’s 6 dimensions of culture

- PDI, IvC, MvF, UAI, LvS, IvR
- Most commonly used cultural framework
- Values 0-100



What about cyber?

- Conscious thought versus unconscious thought.
- How problems are perceived, organized and resolved

Data

- Hofstede's data
 - CSV files contains cultural data for 100 countries across 4 - 6 dimensions (values grouped by thirds)
 - MITRE CAPEC database <http://capec.mitre.org>
 - Zone-H data archives (2005 - 2015) www.zone-h.net or www.zone-h.org
 - 13 million records
 - 1000 actors identified and assigned in other studies
 - 466,220 clean self-identified actors
 - 260, 815 filtered into the CAPEC vectors


A Sample Record

```
IRAN, "2012-01-12 20:48:09", "Team 007 - Persian Defuse HackingTeam 007 - Persian  
n Defuse Hacki", "http://arianadarb.com", "208.66.74.49", "Linux", "Apache", "He  
h...just for fun!", "SQL Injection", "./defaced/2012/01/01/arianadarb.com", "reg  
ular", "no", "published", "homepage", "16504269", "United States"
```

Mirror saved on: 2012-01-01 19:37:37

Notified by: Team 007 - Persian
Defuse HackingTeam 007 - Persian
Defuse Hacki

Domain: http://arianadarb.com

IP address: 208.66.74.49 

System: Linux

Web server: Apache

[Notifier stars](#)

This is a CACHE (mirror) page of the site when it was saved by our robot on 2012-01-01 19:37:37

HACKED OFF!

EZRAIL YAHOO



MAHDI 007

How do we process?

- MWW
- Spearman correlations
- We use these to:
 - Focus and inform the studies that we wish to propose.
 - Check against unfounded claims (i.e. single hacker culture, young single, anti-social male)
 - Gain insights on the 3 types of cyber actors of interest (attacker, defender and victim)

Social Engineering Victims

Year	# Victim Countries	# Non-Victim Countries	# Records Hofstede All attacks	# Records Hofstede "Social Engineering"
2011	55	35	431,758	3723
2012	62	29	310,492	3667
2013	67	27	448,231	5224
2014	70	22	325,137	4460

MWW Results

Yr/Dim	PDI	IvC	MvF	UAI	LvS	IvR
2011	-0.0006	0.0000	0.398	0.02721	0.0184	0.0959
2012	-0.004	0.0034	0.1227	0.0017	0.0003	-0.0575
2013	-0.0123	0.0013	0.0844	0.0669	0.0007	-0.291
2014	-0.0055	0.0028	0.0804	0.0938	0.0367	-0.8021

Social Engineering Victims

Correlations with Population Moderation

Victims /Dim	PDI	IvC	MvF	UAI	LvS	IvR
Victims	+ Mod.	- Mod.	Weak -	None	+ Mod	None

Dimension/ Vector	PDI	IvC	MvF	UAI	LvS	IvR
0 day	High	x	x	x	x	High (R)
BFA	High	x	High	x	x	x
Config.	High	x	High	x	x	x
Mail	High	x	Low (M)	x	x	Low (Res)
Password	High	x	Low (M)	x	x	x
Social Eng. Attackers	High	x	x	High	x	Low (Res)
Social Eng. Victims	Low	High (Ind)	x	x	High (LTO)	x
SQL injection	High	x	x	High	x	x

*Legend: x indicates no statistically significant finding, **P** ≤ 0.05 ; **P** ≤ 0.10

A Word About Defenders

- This data is a bit more difficult to deal with.
- There is one study on DNSSEC, who signed their zones.
- Looking at top level domains (TLDs) was easy. There remains much to be done and would happily work with students on the larger study.
- DNSSEC available since the late 1990s, adoption rates vary.
- Root zone signed in 2010.

DNSSEC Study Findings

MWW Results - TLDs signed

Dim	PDI	IvC	MvF	UAI	LvS	IvR
Signed	-0.0001	0.002	-0.192	0.4602	0.0001	0.4483

Spearman Correlation Results

Dim	PDI	IvC	MvF	UAI	LvS	IvR
Signed	-0.45	0.37	0.09	0.01	0.41	0.02

Tended to be egalitarian,
individualist, long-term oriented.



You hacked my site - now it's payback!!

May be that was not you, but it was someone from turkey...

Now we are even - 1:1.

And, message to all Turk people - stop hacking Serbian sites, or i'm gonna destroy 400 more TR sites!!

Reasons - Pre-Published

Reason	PDI	IvC	MvF	UAI	LvS	IVR
“...be the best”	77	30	50	76	33.5	43
“...challenge”	73.5	31	53	73	42.5	40
“...just for fun”	70	33	54	76	41	42
“Patriotism”	77.5	30	51	72.5	36	42
“Political...”	70	30	53	80	38	44
“Revenge...”	70	30	52.5	75.5	31	42.5
Any Excuse ¹	78	30	53	70	36	32
Hofstede Medians	68	30	46	64	38	47

¹Any excuse indicates the country had actors represented in each reason.

Summary

“This dominance of technology over culture is an illusion. The software of the machines may be globalized, but the software of the minds that use them is not” (Hofstede, Hofstede & Minkov, 2010)



THANK YOU FOR YOUR TIME!

char.sample@icf.com

charsample50@gmail.com

BACK-UP SLIDES

Attack Vectors “Hackmode”

- 0 day - 2009 and the rise of bug bounty programs, Google 2010
- Brute Force Attacks - e.g. password guessing
- Config/Admin Errors - misconfigurations
- Mail
- Password Sniffing
- Social engineering - does not specify which specific attacks
- SQL injection

Distribution of Attacks

Vector	# of Attacks	# of Countries	# Identities
0 day	3,410	21	90
BFA	2,927	21	73
Config	16,820	23	167
Mail	1,993	12	70
Password	184,155	19	142
Social	2,758	17	112
SQL	48,752	35	326

MWW Comparison Findings

Vector	PDI	IvC	MvF	UAI	LvS	IvR
Oday	0.001	-0.288	0.540	0.702	0.819	-0.048
BFA	0.019	0.542	0.005	0.345	-0.449	-0.407
Config	0.002	0.676	0.012	0.776	-0.389	-0.407
Mail	0.039	-0.125	<i>0.072</i>	0.146	-0.2878	-0.176
Pass	0.012	0.261	<i>0.098</i>	0.140	-0.695	-0.271
Social	0.021	0.817	<i>0.052</i>	0.111	-0.482	-0.026
SQL	0.017	0.492	0.172	0.011	-0.500	<i>-0.080</i>