



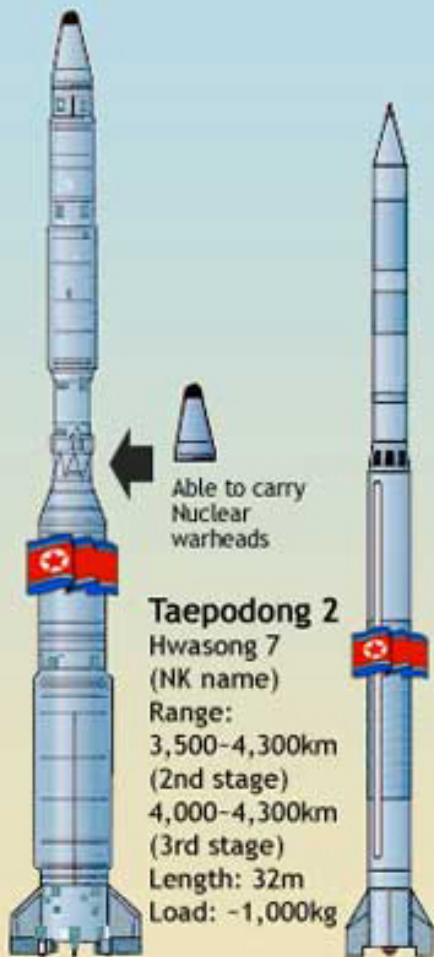
CAPITOL COLLEGE

1927

Cultural and Computer Network Attack (CNA) Behaviors

By: Char Sample & Dave Barnett
CERT & ZScaler

Cyber War Is Here



Taepodong 2
Hwasong 7
(NK name)
Range:
3,500-4,300km
(2nd stage)
4,000-4,300km
(3rd stage)
Length: 32m
Load: -1,000kg



Taepodong 1
Hwasong 6
(NK name)
Range:
1,500-2,000km
(2nd stage)
2,475-2,896km
(3rd stage)
Length: 25m
Load: 1,000kg



Rodong 1
Hwasong 5
(NK name)
Range:
1,000-1,300km
(2nd stage)
Type: single-stage
ballistic missile
Length: 15m
Load: 1,000kg



Scud-C Upgrade
Range: 550km
Type: single-stage
ballistic missile
Length: 11.25m
Load: 500kg



US claims the PC XT can reach the entire internet if equipped with network interface card and access to Internet connection



Able to carry DDoS payloads



IBM PC XT
Range: The internet
Type: Personal Computer
CPU: 8088 @ 4.77 MHz
Memory: 128KB - 640KB

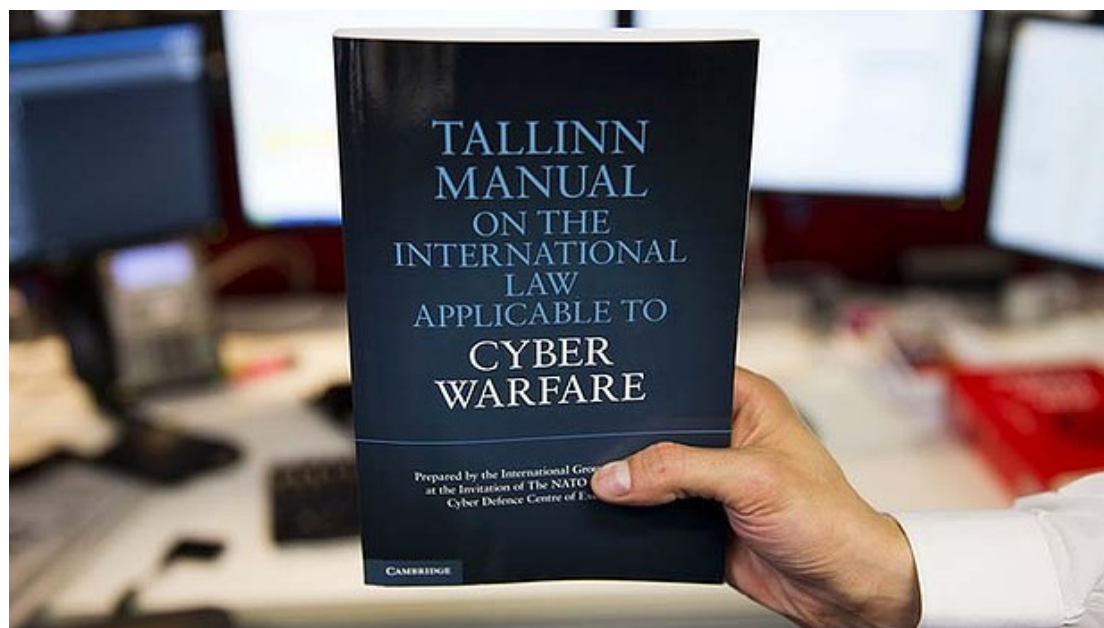




Rules are Being Discussed

1868 St Petersburg Declaration

1949 Geneva Convention



Sometimes Attribution is Obvious...

```
View: mrxnet.sys
C:\Users\kamil\Desktop\stuxnet_malware\mrxnet.sys
:" -i|K D Ç+ Ç+ \FileSystem\cdf s \
&(<@
|
8Lr
8Tr>
8Xr>
QSUW
Nf=0•
f=9•
URPQQh
L$,3
UUWS
SUWj•
UQPXYIYI
ObReferenceObjectByName•
<58763ECF-8AC3-4a5f-9430-1A310CE4BE0A>•
.LNK•
WTR•
.TMP•
\FileSystem\cdf s•
\FileSystem\fastfat•
\FileSystem\ntfs•
RSDS
b:\myrtus\src\objfre_w2k_x86\i386\guava.pdb•
IoCreateDevice•
IoDeleteDevice•
IoRegisterFsRegistrationChange•
ObfDereferenceObject•
IoDriverObjectType•
```



CAPITOL COLLEGE

1927

...Sometimes Not





We Need New Methods

- **What:** We are trying to find a non-technical way to understand where an attack originates from.
- **Why:** to allow us to better analyse the consequences of an attack and be able to take appropriate action
- **To answer the question:** “Who did this to me?”





CAPITOL COLLEGE

1927

Here's a thought...

What if people subconsciously left their fingerprints in an attack?



Conscience vs Unconscious Thought

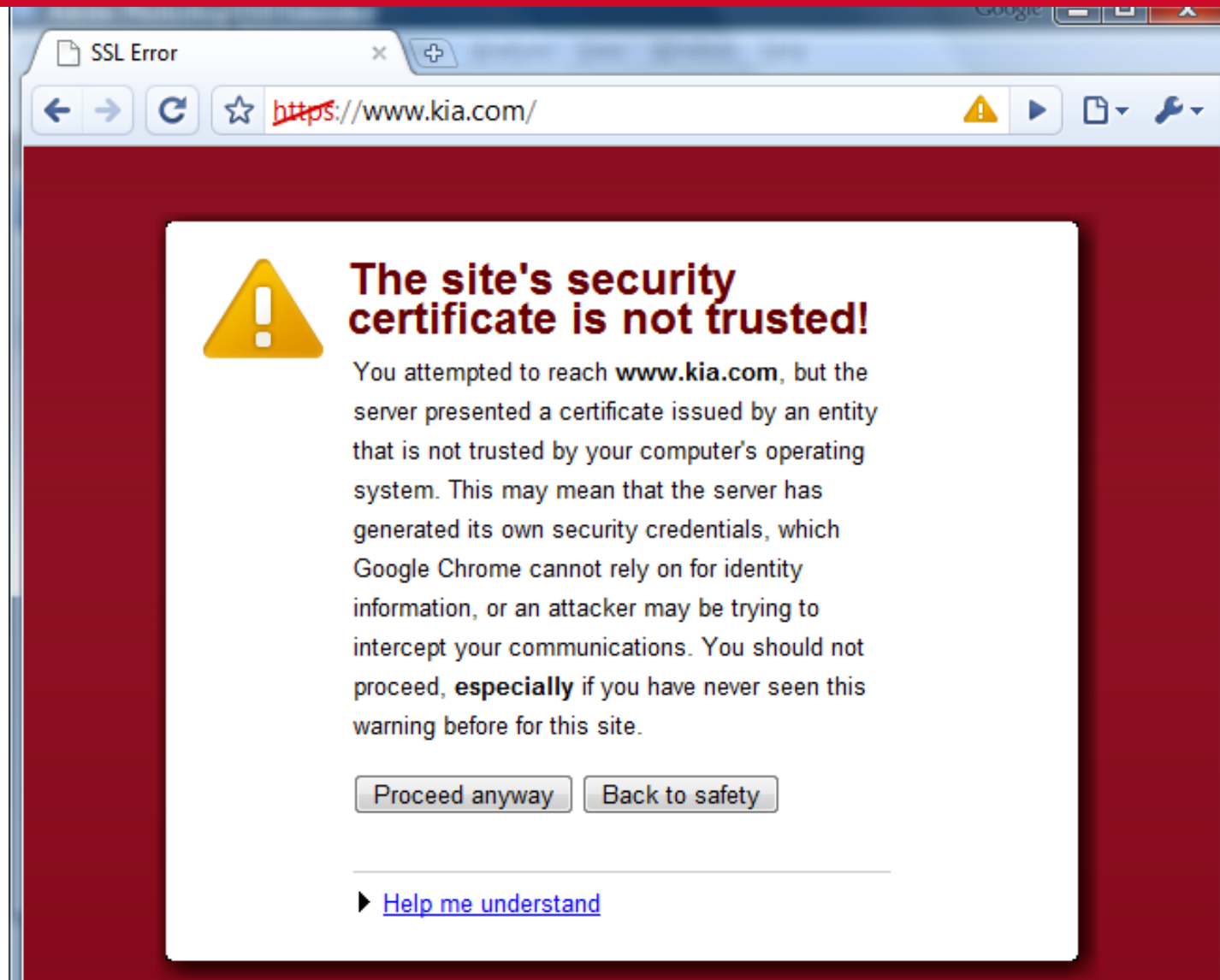
40-60 bps.



11,000,000 bps.



Conscience vs Unconscious Thought





Put it another way!

System 360



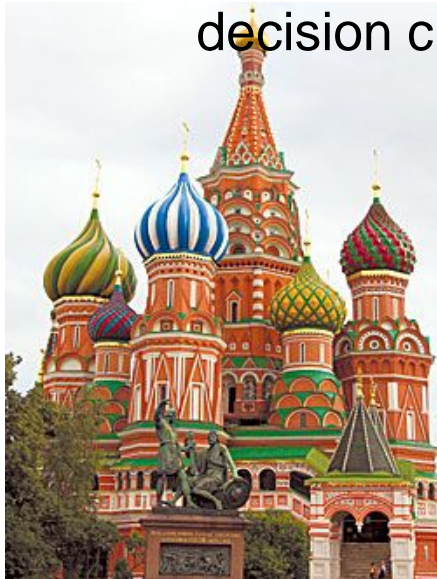
Google



People CAN NOT fool their unconscious

Cultural Studies

- Hofstede, Hofstede & Minkov
 - Definition of culture: “the collective mental programming of the human mind which distinguishes one group of people from another”.
- Dr. Dominick Guss
 - Culture influences problem perception, strategy development and the decision choices.



6 Cultural Dimensions

- Power distance:
- egalitarian vs hierarchy



- Individualism:
- individual vs collective



- Masculinity:
- masculine/feminine roles



6 Cultural Dimensions

- Uncertainty avoidance:
 - fear of the unknown



- Long term orientation
 - delayed vs immediate goals/results.



- Indulgence vs restraint
 - fun vs self-restraint



Research Plan

- Extract countries of origin from reports of specific website defacements for comparison against Hofstede's data.
 - Hypothesis Tests:
 - There is no relationship between high PDI values or any other dimensional values and nationalistic, patriotic themed website defacements.



Presidencia Española eu trios.es

Search:

HOME THE SPANISH PRESIDENCY AGENDA DOCUMENTS & NEWS THE EUROPEAN UNION SPAIN IN FOCUS PRESS

You are here : Home

• The Spanish presidency
• Agenda
• Documents & News
• The European Union
• Spain in focus
• Press

TOP SEARCHES

Noticia UE Bruselas UE
Política Presidencia Cultura
Política Cultura

Resultados de búsqueda

|| No se han encontrado Resultados ||

Error

org.openrsr.search.OneSearchException: Búsqueda de 'query['

Agenda

JANUARY, 2010

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

See the calendar for:
(European Council) ok



CAPITOL COLLEGE

1927

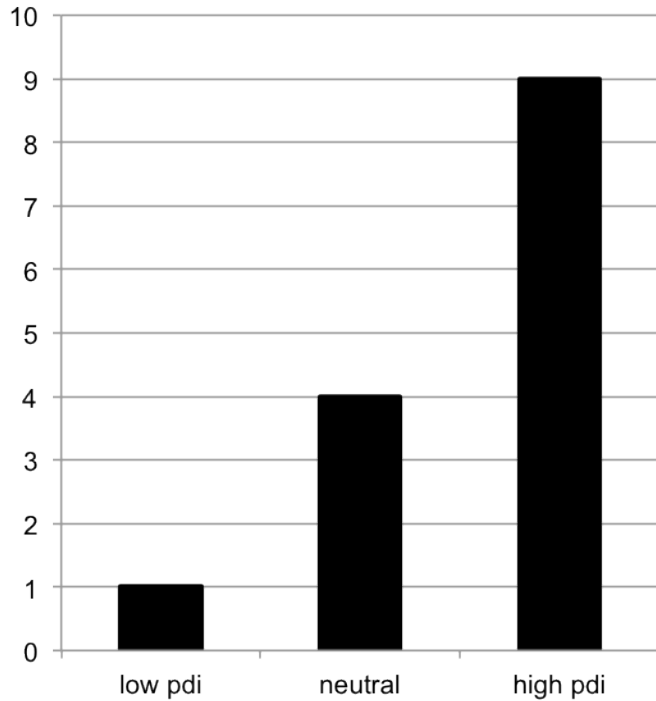
The question

- Hypothesis Tests:
 - Easier to disprove a null.
 - Rules for considering alternative/
 - Same test for each dimension.

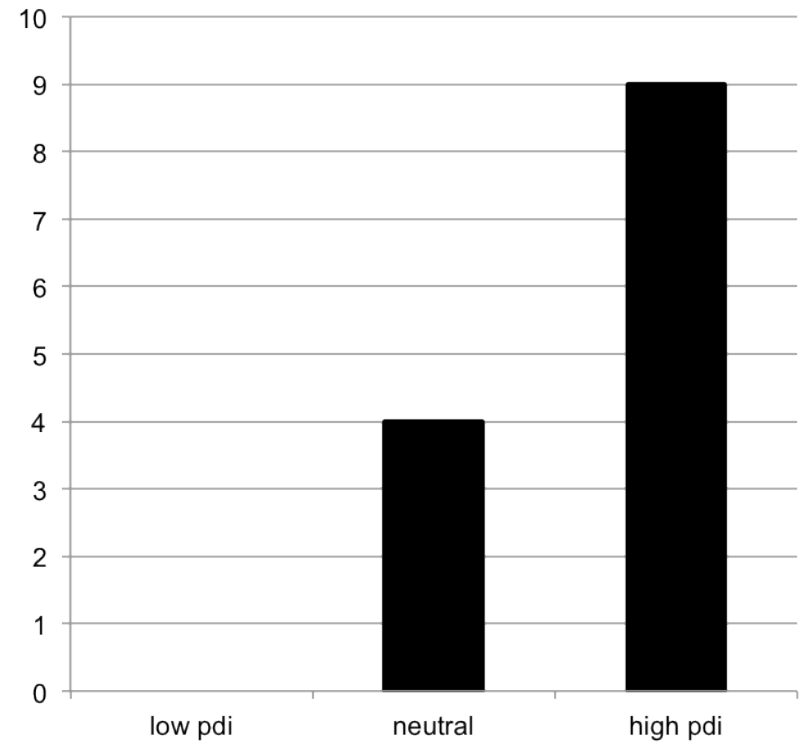


Results – PDI

PDI With Israel



PDI Without Israel

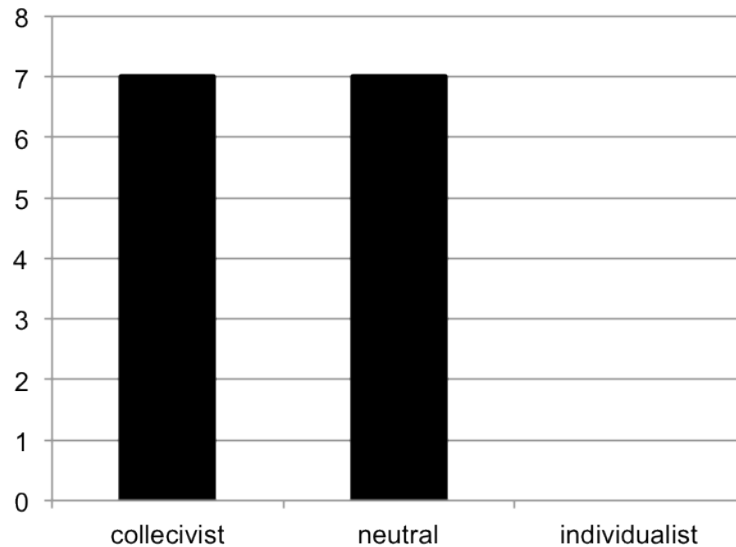


Results – IVC

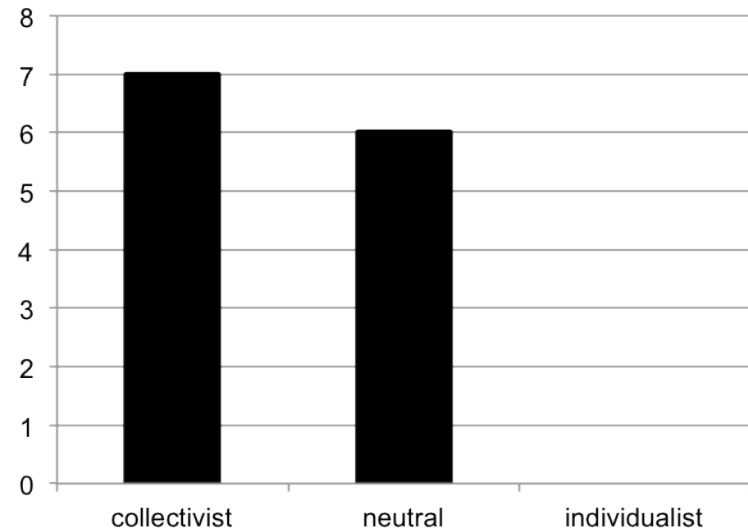
IVC With Israel

IVC Without Israel

IVC Results



IVC Results without Israel





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.
 - Change focus to examine for cultural traces in other activities such as software coding.
- Conclusions
 - Culture does appear to influence attack behaviors.
 - Further research is needed.
 - Understand the role of each dimension’s role in cyber attacks.
 - Understand how this work fits with other efforts in cyber research.



CAPITOL COLLEGE

1927

Thank You!

Q & A



BACKUP SLIDES

- Unconscious thought
 - Dijksterhuis (2004): Unconscious thought does more processing than does conscious thought.
 - Conscious thought, single threaded approximately 40-60 bps.
 - Unconscious thought: multi-threaded approximately 11,000,000 bps.
 - Evans (2008): Speed of unconscious thought differs from speed of conscious thought. “Consciousness is also inherently slow, sequential, and capacity limited.”
 - Bargh and Morsella (2008):
 - “In nature, the ‘unconscious mind’ is the rule, not the exception.”
 - “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”.
 - Gifford (2005) - Past events help to form future perceptions. (On-going Bayesian process)
 - Matching bias
 - Belief bias
 - 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.



Literature Review

- Hofstede, Hofstede, and Minkov (2010)
 - Definition of culture: “Culture is defined as the *collective mental programming of the human mind* which distinguishes one group of people from another.”
 - Six dimensions of culture
 - Culture throughout life
 - Family
 - Education
 - Cognition
 - Technology
 - At work

Results (1)

Results of Question One Test Without Israel

Hypothesis #	Test	Tool	U=	Z=	p-value	Accept/Reject
(PDI) $H1_0, H1_1$	$\mu \leq 59$	Mann-Whitney	293	2.42	0.0078	Reject
(IVC) $H1_0, H1_2$	$\mu \geq 45$	Mann-Whitney	714.5	-2.35	0.0094	Reject
(M/F) $H1_0, H1_3$	$\mu \geq 50$	Z Test	n/a	0.5714	0.4247	Accept
(UAI) $H1_0, H1_4$	$\mu \leq 68$	Mann-Whitney	24.5	-1.33	0.0918	Accept
(LTO) $H1_0, H1_5$	$\mu \leq 45$	Mann-Whitney	500	1.15	0.1251	Accept
(IVR) $H1_0, H1_6$	$\mu \geq 45$	Mann-Whitney	786	-1.51	0.0655	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.