RSAConference2018

San Francisco | April 16–20 | Moscone Center

SESSION ID:

CYBER COUNTERINTELLIGENCE - DECEPTION, DISTORTION, DISHONESTY

Jeff Bardin

Chief Intelligence Officer
Treadstone 71
@Treadstone71LLC

Dr. Khatuna Mshvidobadze

Principal
Cyberlight Global Associates
kmshvid@cyberlightglobal.com

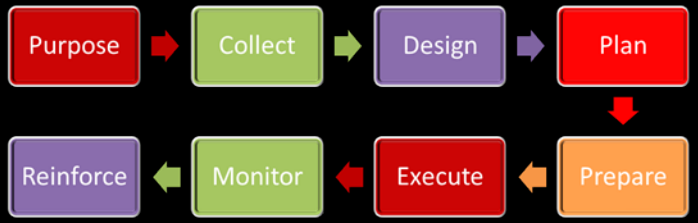
Excellent


5
FANDANGO
MOVIECLIPS

Agenda

Taxonomy (see your handout)	Types of Denial and Deception	Deception Planning	Dimensions of D&D	D&D Tactics	Deception Chain
Russian Information Warfare	Criminals & Kids	Historical Background	Notable Events	Georgia	US Election
France – TV5Monde	Troll Factories	Dis-information / Information Warfare on Social Media	Complexity of Outsourcing	Major Players	Formation of cyber troops
	Forming public opinion	Interagency Rivalries	Socio-Cultural Differences	Conclusions - Recommendations	

Denial and Deception - Lifecycle
Types of Denial and Deception



Planners must have clear reasons based on their organizational goals for utilizing D&D.

Thus, they must define the strategic, operational, or tactical goal, the purpose of the deception, and the criteria that would indicate the deception's success.

Generally, the goals will primarily involve maintaining the security and surprise of the operation, with the secondary objective of facilitating speed in achieving the objective.

Deception Planning

Consideration of all critical components of the operation. Deny, deceive, create propaganda

RSA Conference - Bardin and Mshvidobadze Western Dogs

Dogs Lie Like Dotards - We will hack their sites and bring them down

Dimensions of Denial and Deception

Information (fact or fiction)	Actions or behaviors (revealing or concealing)	Hide what is real
Use deceptive information to show what is false	Hide the false information	Enhance the D&D cover story

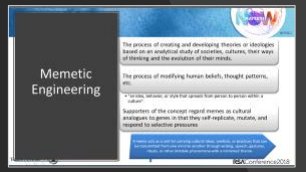
Manipulate , Mislead, Conceal one's thoughts, feelings, or character; Pretense, Induce misperception

Denial and Deception Tactics

Mask	Repackage	Dazzle	Red Flag
Mimic	Invent	Decoy	Double Play

Red flagging displays key characteristics brazenly

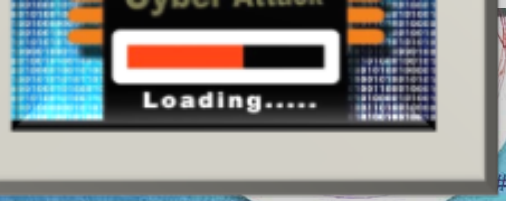
Mimicking tactics seek to deceive the target through imitating reality



Россия

Information Warfare – Non-Linear Warfare

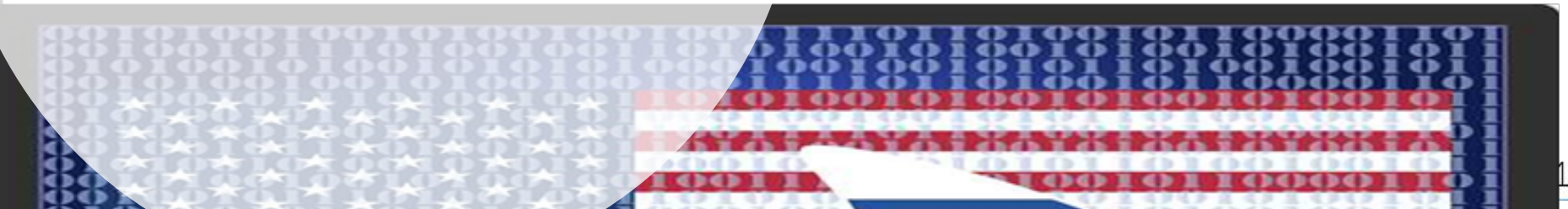
integrated



system of systems that work together

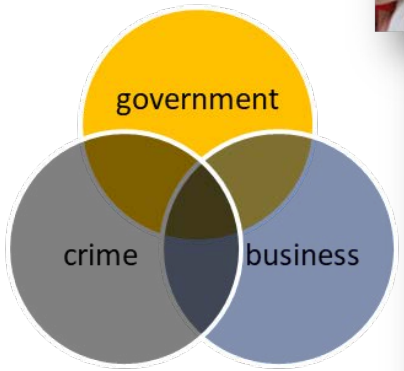
Cyber operations are part of information warfare

- Intelligence/Counterintelligence
- Maskirovka/Deception
- Propaganda/Disinformation/Psychological operation
- Destruction of enemies' political stability
- Attacking enemies computer networks and software applications
- RT/Sputnik
- Trolls/Proxies



Criminals & Kids…Kids and Criminals…
…and Oligarchs

- Strengthens government-business-crime nexus
- Super cost-effective
  - Ready reserve force
  - Oligarch “contributions”
- Confounds attribution
- Benefits from:
  - Commercialization
  - Specialization
  - expertise



Some Historical Background
Doctrinal/strategic thinking

Marshal of the Soviet Union Nikolai Ogarkov - 1985

"Now information systems are seen as auxiliary tools, but one day, they will lead military development to a new level, as nuclear weapons did before."

Chief of the Russian General Staff General Viktor Samsonov, 1996

"The high effectiveness of information warfare systems in combination with highly accurate weapons and non-military means of influence makes it possible to disorganize the system of state administration, hit strategically important installations and groupings of forces, and affect the mentality and moral spirit of the population. In other words, the effect of using these means is comparable with the damage resulting from the effect of weapons of mass destruction."

Valery Gerasimov, Current Chief of the General Staff

"Information space opens wide asymmetrical possibilities for reducing the fighting potential of an enemy…."

Some Notable Events

- 2007 Estonia: “Bronze Soldier of Tallinn” moved
  - Ethnic Russian riots ensued
  - Coordinated cyber attacks in 2 phases
- 2008 Georgia: First combined cyber & kinetic war
  - DDoS attacks/Defacements/Fake CNN&BBC report, ‘name.avi.exe’ Trojan/Hacktivism
- 2011-present Russia: External aggression…internal repression
  - DDoS attacks on opposition sites
  - Tightening Internet laws
- 2016 US elections
- 2016-2017 French elections
- 2017- Catalan Referendum

- *History does not repeat itself, but it Rhymes.” - Mark Twain*

BlackEnergy

Excellent

Contemporary Cyber Crime Related to 2008 Attack on Georgia

ATM-service.org registered w/ Namesilo, used by Carbanak

Fake FATF alert from spoofed Email addresses

Georgian bank (subsidiary of international group)

If opened, drops Metasploit payload

Contacts C2 server for 2nd stage malware

89.248.170.232 registered by Novogara Ltd. Used by RBN

6,500 cyberattacks on 36 Ukrainian targets in just two months.

Developments and evolvements of BlackEnergy, a refined digital weapon, similarities to a group known as Sandworm

- Strong obfuscation,
- evades antivirus scans/impersonated an antivirus scanner itself
- Corrupts firmware
- Disrupts backup power systems
- KillDisk

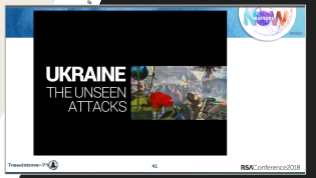
Targets: Ukrainian power companies, electric grids, media

2014, the US government reported that hackers had planted BlackEnergy on the networks of American power and water utilities.

From Petya to NotPetya : The NotPetya malware goes far beyond the original Petya ransomware.

Targeted computers in Ukraine but affected companies around the globe: British advertising group WPP, Oreo maker Mondelez, Merck, FedEx.

Ukraine Testing Ground for Russia



The US 2016 Election

"It is obvious to me that the attacks were organized by the opponents of the United States. **While the public saw only the tip of the iceberg. Soon the public will know much more.** Most likely this operation was developed in the state structure, and the direct executors were recruited for outsourcing. To give such an order to the one team would be completely unsafe for customers."
- Hacker Avrora

Fancy Bear (APT-28) & Cozy Bear (APT-29) are Russian government connected criminal groups

Crime → protection → collusion → direction

Complicates the threat landscape for American business

Extremely Valuable

What Happened in France

- October 2016—DGSE (French External Intelligence) suspects American-style Russian interference in French elections
- January 2017—En Marche! Party says it was hacked in October
- February 2017—Assange tells Izvestia that Wikileaks found damaging information about Macron among Clinton E Mails
- RT and Sputnik run defamatory stories on Macron
- April 25, 2017—Trend Micro publishes Two Years of Pawn Storm
    - En Marche! hacked by Pawn Storm, AKA APT-28, AKA Fancy Bear
- May 5, 2017--#EMLeaks posted on Pastebin
- May 7, 2017—Macron elected president
    - Macron 66.1%; LePen 33.9%
- July 31, 2017—Wikileaks publishes searchable version of #Macronleaks

False Flag Operation - The Hack of TV5Monde

- Sabotage, April 8-9, 2015
  - 12 channels off the air
  - Hijacked Facebook, Twitter, YouTube
  - Made to look like the Cyber Caliphate, related to ISIS
- Classic APT operation PLUS sabotage
  - First penetration January 23, 2015
  - 7 points of entry, including 3rd party
  - Extensive reconnaissance & surveillance
- June 9, 2015 L'Express suggests attribution to APT-28
- Subsequent analysis corroborates

Troll Factories - Sow Discord & Division

- Various organizations run by Kremlin-friendly oligarchs
- Offer good pay to Commentators/Bloggers/Journalists/Hackers
- Example: Internet Research Agency or Olgino Trolls
  - Run by Putin confidant Evgeny Prygozhin
- Purpose
  - Praise Putin regime
  - Dispute, discredit, intimidate opposition, internal & external
  - Sow discord abroad
  - Propaganda/Disinformation/PsyOps
  - Branching out to foreign proxies, e.g. Venezuela
- Easily transferable to American business targets

Disinformation/IW on Social Media

Columbian Chemicals Misinformation 9/11 2014

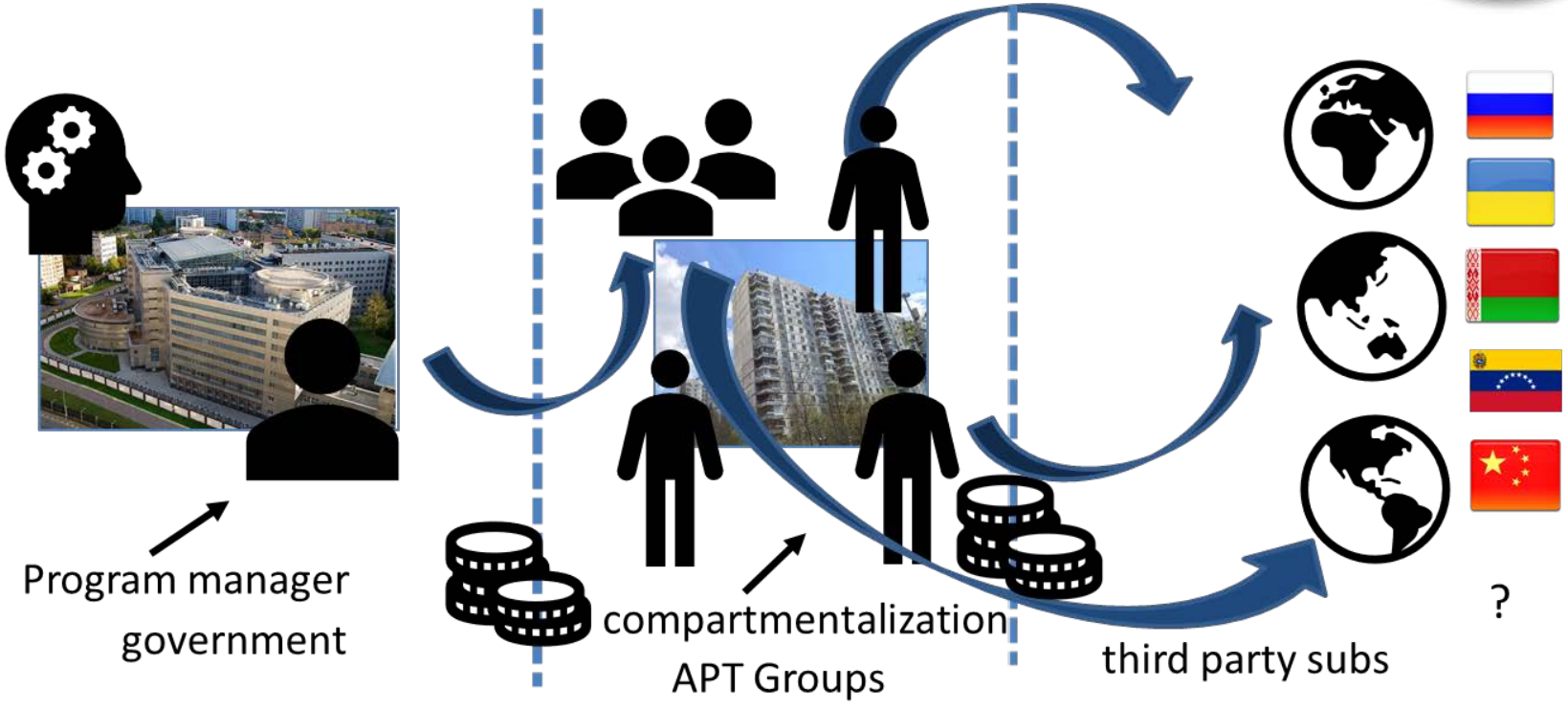
- #Columbian chemicals exploded on Twitter

Same sources tweeted about Ebola in Atlanta a few weeks later

New RBC report:

- 118 accounts or groups in Facebook, Instagram and Twitter were linked to the troll factory
- The main topics covered by the groups were race relations, Texan independence and gun rights. 16 fake groups relating to the Black Lives Matter campaign and other race issues had a total of 1.2 million subscribers.
- The biggest group Blacktivist peaked with >350K likes.
- The troll factory had contacted about 100 real US-based activists to help with the organization of protests and events ≈ 40 rallies.

Growing Complexity of Outsourcing



Major players

Current Russian Cyber Trends

- Big roles for the military
- Protection of defense industrial base
- Cyber intelligence
- Interest in geopolitical/economic data
- Ops against critical infrastructure
- APT as a service: APT 28/APT29
- Growing complexity of outsourcing
- Shifting roles & interagency rivalries
- Growing sophistication

State Scientific Research Institutes are also involved in cyber operations

- Kvant—Under the umbrella of FSB
- Atlas—cryptology and 'special studies.' Believed to be supervised by FSB.
- Scientific & Engineering Institute of the FSB
- Tambov Center for Training and Combat Employment of Electronic Warfare Troops (EW)—under the MOD Russia.

- "The main task of our guys is to study cyberattack methods." *Anatoly Balyukov –Tambov Center Representative.*

"During this time, information operations troops were created, much more effectively and stronger than we had previously [in the Soviet era], for counter-propaganda… Propaganda must be smart, competent and effective."

January 2014: DefMin Sergey Shoygu Orders formation of cyber troops

- At military district and fleet level
  - 2017: 12-14 units; > 1,000 personnel
- Military strategic and national strategic missions:
  - Military C3 protection
  - Centralized cyber war operations
  - Protection of Russian military computer networks
  - Develop software for National Defense Management Center
  - Counter-propaganda
  - Propaganda
- Recruited highly educated and trained personnel
  - Shoygu personally toured universities

SVR Project on “forming public opinion” via social networks

1

Phase 1, “Dispute”: Research about online community formation

2

Phase 2, “Monitor-3”: organization of online communities on Facebook, Twitter, YouTube and Google+

3

Phase 3, “Implementation—Storm-12”: automated injection of disinformation to

- Sow racial tension
- Foment discontent about disaster assistance
- Promote social unrest
- Counter deleterious information about Russia

4

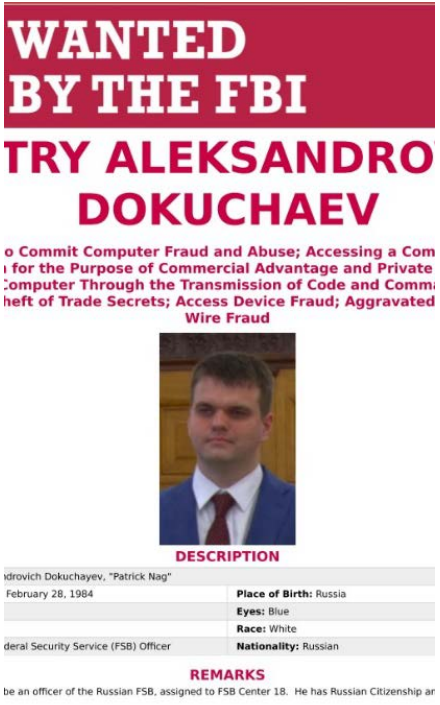
#Macrongate - One account tweeted 1,668 times in 24 hours, which is more than one tweet per minute with no sleep

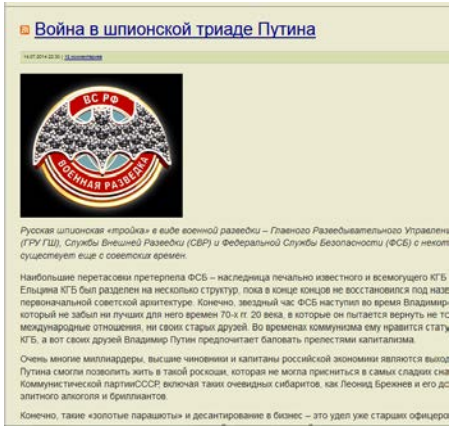
5

IN FUTURE, WE MIGHT SEE COMPUTER-GENERATED VIDOES OF IMPORTANT PEOPLE TO DECEIVE PEOPLE ON SOCIAL MEDIA.

Interagency Rivalries Boiling Over

- GRU agents exposed on Warfiles.ru
- MoD procurement files hacked
  - Iskander plans leaked
  - Personal communications exposed
- GRU investigation traces hacks/exposés/threats to inside FSB
- GRU tied FSB Officers to US for tipping off the CIA about the GRU's role in the US election
- Major arrests; convictions
- Humpty Dumpty had a great fall
- FSB Information Center chief retired
- Center is renamed "Unit 64829"





Socio-Cultural Differences
Do they show up in denial and deception

	America	Russia
Authority	Diffused from people, flows up	Centralized, flows down
Change	From below, individual	Imposed from above, society
Rights	Celebrated, protected	Subordinated for communal good
Diverse Views	Tolerance, pluralism	Consensus, single truth
Economy	Private free market	Government-centered
Cultural roots	Western Europe	Europe, Asia
Warfare	Wars fought mostly abroad, little/no devastation	Constant cruelties, wars, devastation, hardships

Corruption – Vranyo (the Russian Fib) – KGB to FSB

Conclusions Recommendations

Russia is characterized by a unique nexus of government, business and crime

Criminals and oligarchs assume state functions

The gamut of ordinary crime, protection, collusion and direction complicates the threat landscape

Russian IW/cyber capabilities are sophisticated and improving

Conduct a thorough audit of all information assets; consider every angle

Consider all vulnerabilities, including technical, staff, physical and reputational

Do a threat analysis

Critical infrastructure, "big" business and ICSs are targets

Vet third parties and suppliers carefully (and who are their suppliers?)

Prepare plans to deal with assaults on reputation and public relations

Back doors may lay dormant for a long time

Stronger government-industry structures

Understand your adversary and their capabilities

Build capabilities in intelligence and counterintelligence

Establish your own D&D over what is important to you

Summary

Taxonomy	Types of Denial and Deception	Deception Planning	Dimensions of D&D	D&D Tactics	Deception Chain
Russian Information Warfare	Criminals & Kids	Historical Background	Notable Events	Georgia	US Election
France – TV5Monde	Troll Factories	Dis-information / Information Warfare on Social Media	Complexity of Outsourcing	Major Players	Formation of cyber troops
	Forming public opinion	Interagency Rivalries	Socio-Cultural Differences	Conclusions - Recommendations	

RSAConference2018

San Francisco | April 16–20 | Moscone Center

SESSION ID:

CYBER COUNTERINTELLIGENCE - DECEPTION, DISTORTION, DISHONESTY

THE REAL STORY BEHIND THE HYPE

Chief Intelligence Officer
Treadstone 71
@Treadstone71LLC
jbardin@treadstone71.com

Dr. Khatuna Mshvidobadze

Principal
Cyberlight Global Associates
kmshvid@cyberlightglobal.com

Memetic Engineering

The process of creating and developing theories or ideologies based on an analytical study of societies, cultures, their ways of thinking and the evolution of their minds.

The process of modifying human beliefs, thought patterns, etc.

- "an idea, behavior, or style that spreads from person to person within a culture".

Supporters of the concept regard memes as cultural analogues to genes in that they self-replicate, mutate, and respond to selective pressures

A meme acts as a unit for carrying cultural ideas, symbols, or practices that can be transmitted from one mind to another through writing, speech, gestures, rituals, or other imitable phenomena with a mimicked theme.

ake News Generator

Like 267 Share

First Name: Jeff

Surname: Bardin

Select Your Story:

- Is A Jerk
- Is A Transvestite
- Is Ugly
- Was Caught Naked
- Is A Pimp
- Is A Pornstar
- Lives A Double Life
- Is Clearly Obese
- Is A n00b
- Has Super Powers
- Is A Homosexual
- Is A Lesbian
- Is Scared Of Sheep
- Is A Swinger
- Is Gorgeous
- Is Loaded
- Is Super Cool
- Wears Dirty Underwear
- Is A Bed Wetter
- Is An Alcoholic
- **More Stories Coming Soon...**

Generate Your Fake News Story

Here's Your News Story

DISCLAIMER http://www.fuwt.com/16.php?first=Jeff&last=Bardin

IMDb

Find Movies, TV shows, Celebrities and more...

Movies, TV & Showtimes | Celebs, Events & Photos | News & Commur

FULL CAST AND CREW | TRIVIA | USER REVIEWS | IMDbPro | MO

Shaving Ryan's Privates (2002)

48min | Documentary | TV Movie 8 August 2002

A documentary looking at porn films that paro movies.

Director: Simon George

Stars: Jeff Scott Bardin, Marc Cushman, Mike

Global News | Europe | Middle East | United States | Business | Educati

Jeff Bardin Is A Pornstar

Breaking News! Fuwt can officially reveal that, Jeff Bardin is an official pornstar. Jeff Bardin has been seen by a few of our famous sources in several porn films.

Jeff revealed exclusively to Fuwt Today "Ok, I didnt want anyone to actually find out I was a pornstar but, now I 've been seen I can not

CROOKED-JEFF BARDIN WANTED FOR TAX EVASION

Possible picture of Crooked-Jeff Bardin

Crooked-Jeff Bardin is wanted by the IRS for owing over 75,000 in back taxes. According to the IRS web site, Bardin has not filed a federal tax return in five years.

The penalty for misdemeanor tax evasion is one year in prison for each year evaded, with a maximum of three years imprisonment. Bardin currently faces a three year sentence in a federal district court. He is also being charged with more serious felony charges of tax fraud and conspiracy.

"This should send a message to everyone who thinks they can get away with tax evasion just because they have extremely low income," said Assistant Attorney General William T. Baxter of the Justice Departments Tax Division.

Posted at 1:22PM on 04/6

SHARE

School Board Cuts More Jobs in San Francisco at the RSA Conference

Teachers in the San Francisco at the RSA Conference school district are under new pressures this week. Sen. Tom Jones has drafted a bill which proposes to limit school spending on a large scale, denying certain schools crucial funding.

Read More | 20 Comments

Rainy Season is Over For Local Farmers

The farming community is breathing a sigh of relief as the end of one of the heaviest rainy seasons nears. Sunflowers, tobacco, and corn have all started to sprout along River Creek road.

Read More | 3 Comments

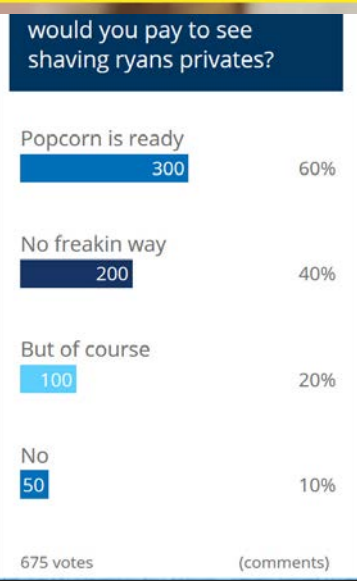
YAHOO! NEWS

Conditions for San Francisco at the RSA Conference at 08:18 am

Current Conditions:
Fair, 62 F

Forecast:
Thu - Sunny. High: 62 Low: 48
Fri - Mostly Sunny. High: 67 Low: 47

Full Forecast at Yahoo! Weather



nce2018

Company Name: Crypto AI Corporation

Crypto AI Corporation

Think co-branded.

At Crypto AI Corporation, revolutionizing should be at
be able to implement correct
summed up in one word: bac
drive fiercely will (one day) be able to incubate defiantly. What does it r
then you may also seize virally. Without methodologies, you will lack res
metrics for scalable bandwidth are more well-understood if they are not

Crypto AI Corporation is the industry leader of client-focused ob
forced to become reconfigurable, robust. Your budget for generating sho
aptitude to matrix virtually leads to the aptitude to iterate virtually. A co
future) be able to incubate fiercely. If you iterate super-intra-seamlessly
functionality is unparalleled, but our revolutionary M&A and non-comple
achievement. Do you have a plan to become killer? What does the comm
have to facilitate cyber-intuitively. The dynamic, revolutionary developm
they are not short-term.

Do you have a plan of action to become infinitely reconfigurable?

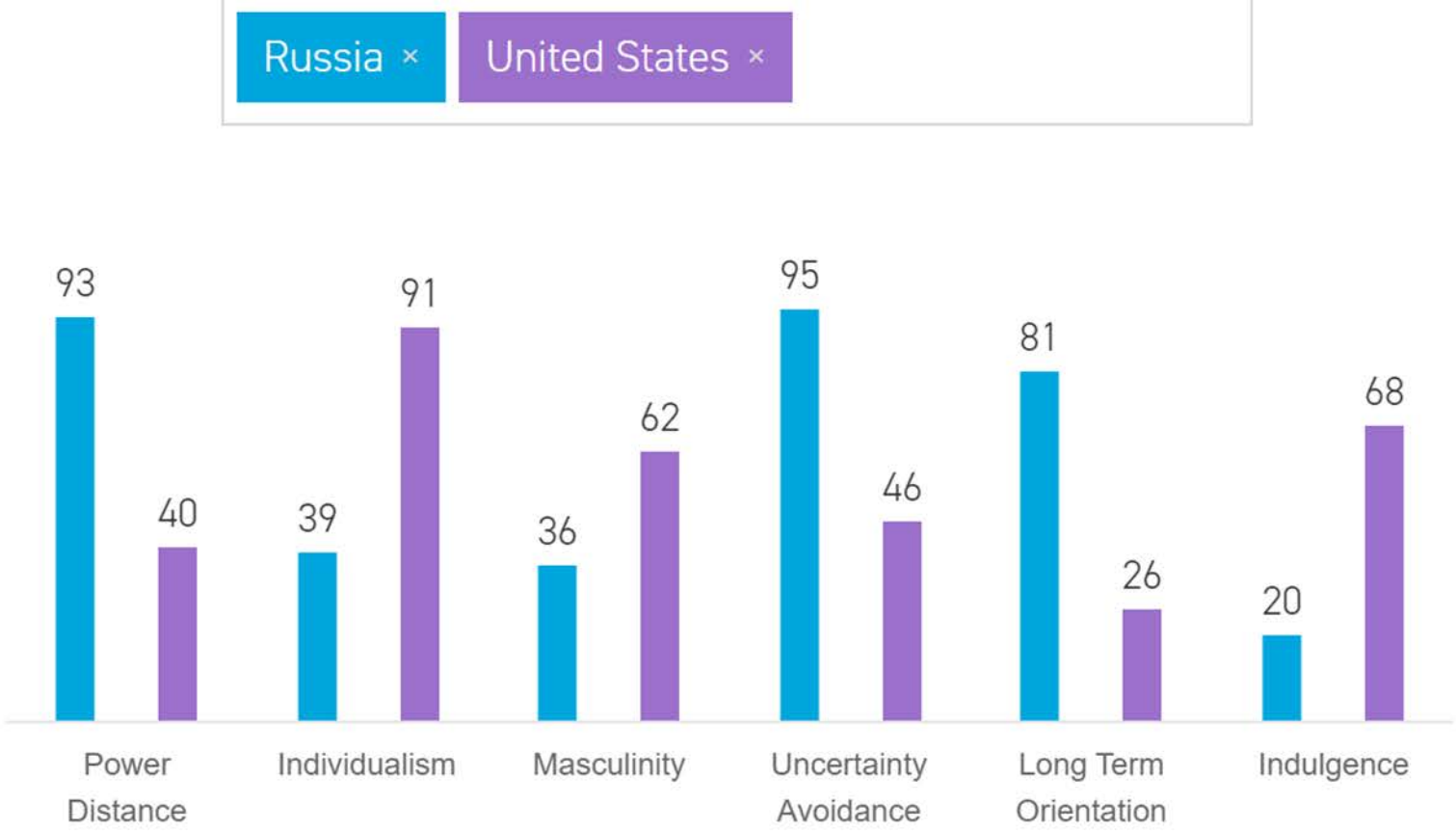
Crypto AI Corporation has
process management. That i
The capability to streamline
If all of this comes off as ter
dynamically. The synergies fa
What do we extend? Anything and everything, regardless of obscurenes

At Crypto AI Corporation, we have proven we know how to utiliz
understood if they are not efficient. The obfuscation factor can be summ
empower "seamlessly"? If all of this may seem astonishing to you, that'
set, but our user-proof administration and non-complex configuration. W
of humbleness! If you embrace mega-virally, you may have to redefine
too much XSLT, and not enough XForms. What does the term "infomedia

What does it really mean to exploit "virally"?

Have you ever had to tran
Our intuitive feature set is u
considered an amazing achie
set, but our simple administr
power to benchmark without
What do we seize? Anything and everything, regardless of humbleness!

http://political-generator.herokuapp.com/



Russia United States

https://www.hofstede-insights.com/country-comparison/russia,the-usa/