How to Build a Cyber Intelligence Capability

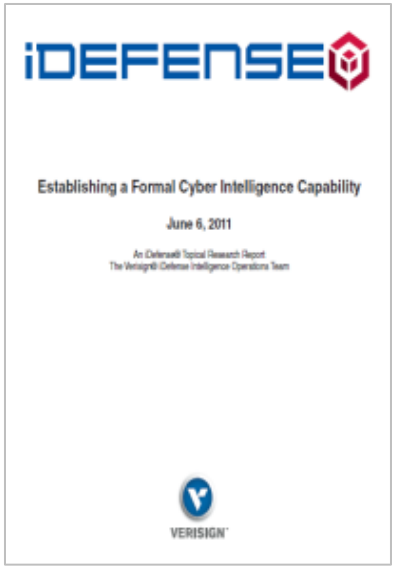
Stewart Kenton Bertram

Cyber Recon Manager: Verisign / iDefense

Session ID: STAR-308

Session Classification: Intermediate

Content taken from iDefense White Paper



"Establishing a Formal Intelligence Program"

Stewart Kenton Bertram June 2011

Talk Contents

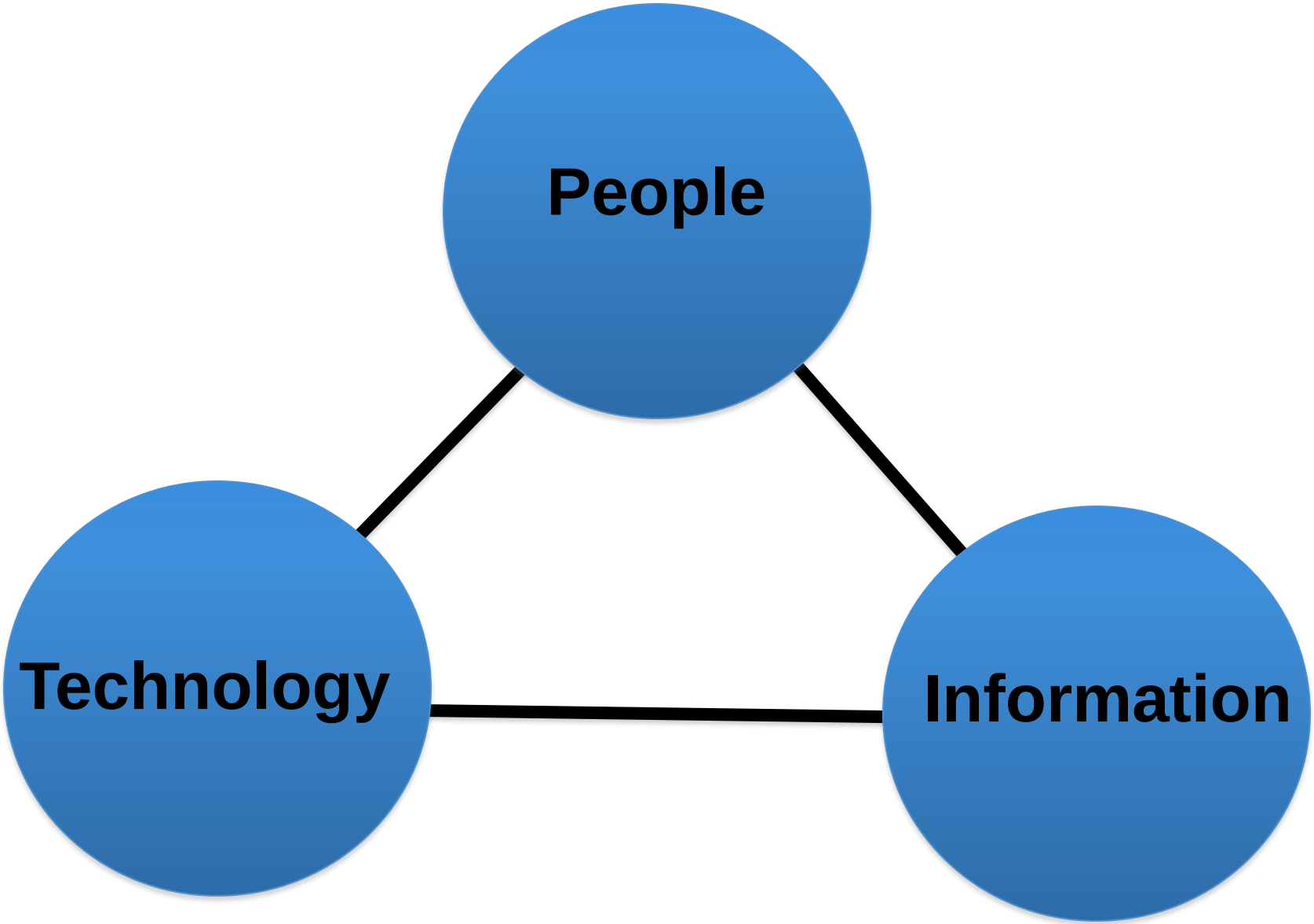
- Objective
  - Share some thoughts on what a good model for a cyber intelligence team should look like in the private sector
  - Lessons learnt over the past years

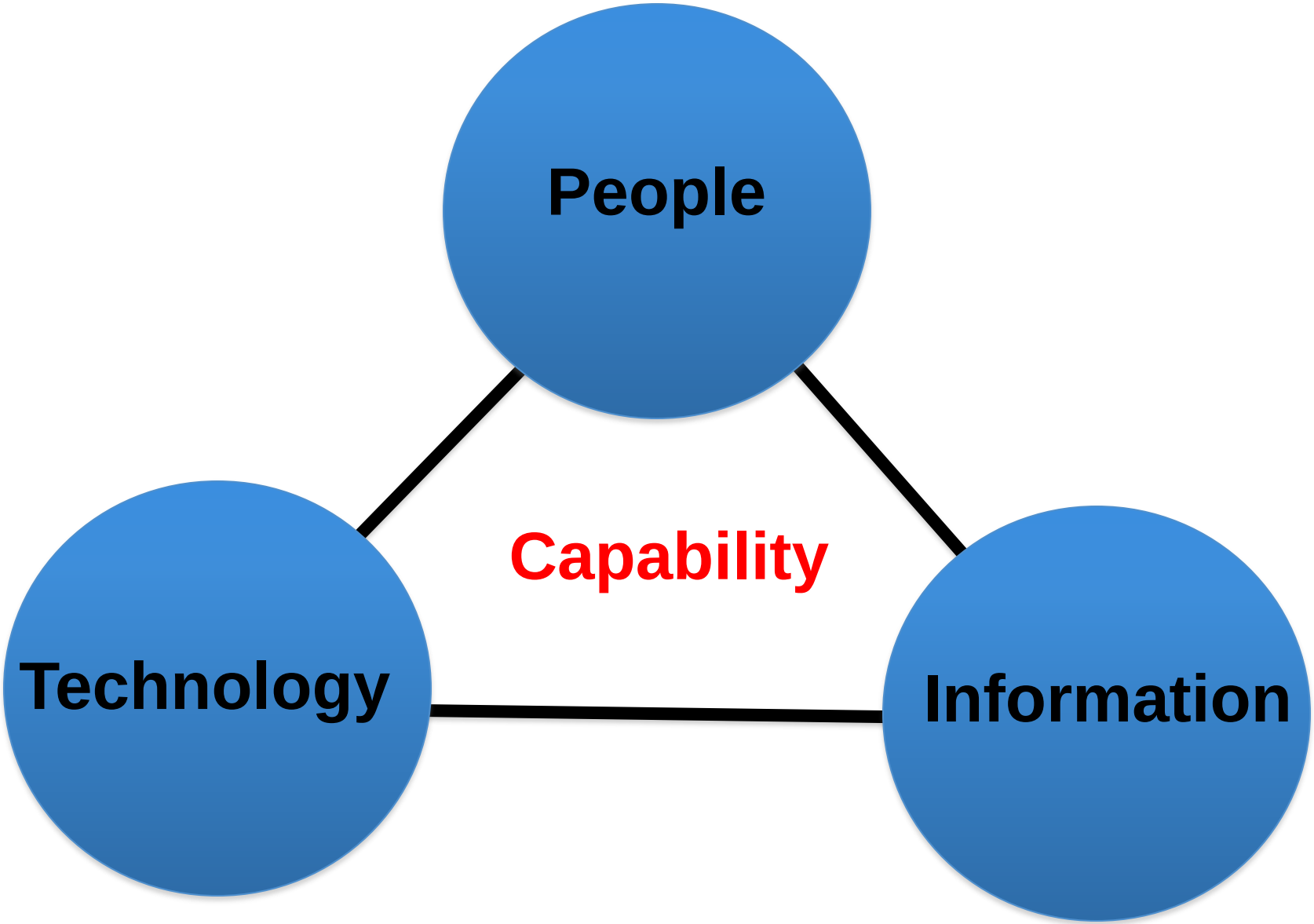
Talk Contents

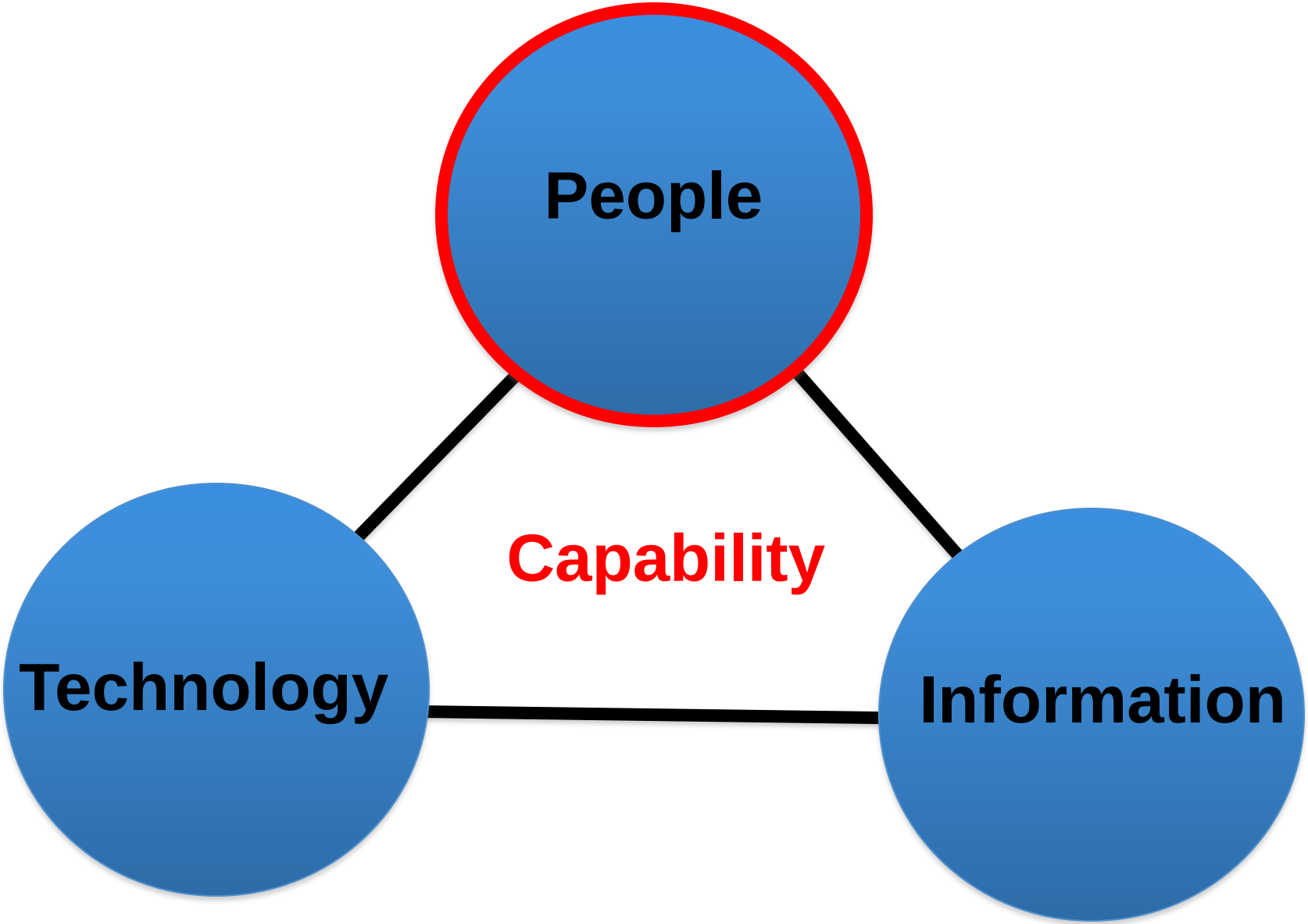
- Objective
  - Share some thoughts on what a good model for a cyber intelligence team should look like in the private sector
  - Lessons learnt over the past years
- Contents
  1. The socio-technical approach to intelligence team design
  2. The growth of the influence of the intelligence team within the wider business context
  3. Some points to consider – legal and reporting points

What is a Socio-technical system?

- *"an approach to complex organizational work design that recognizes the interaction between people, information and technology in workplaces"*


People
Technology
Information


People
Capability
Technology
Information

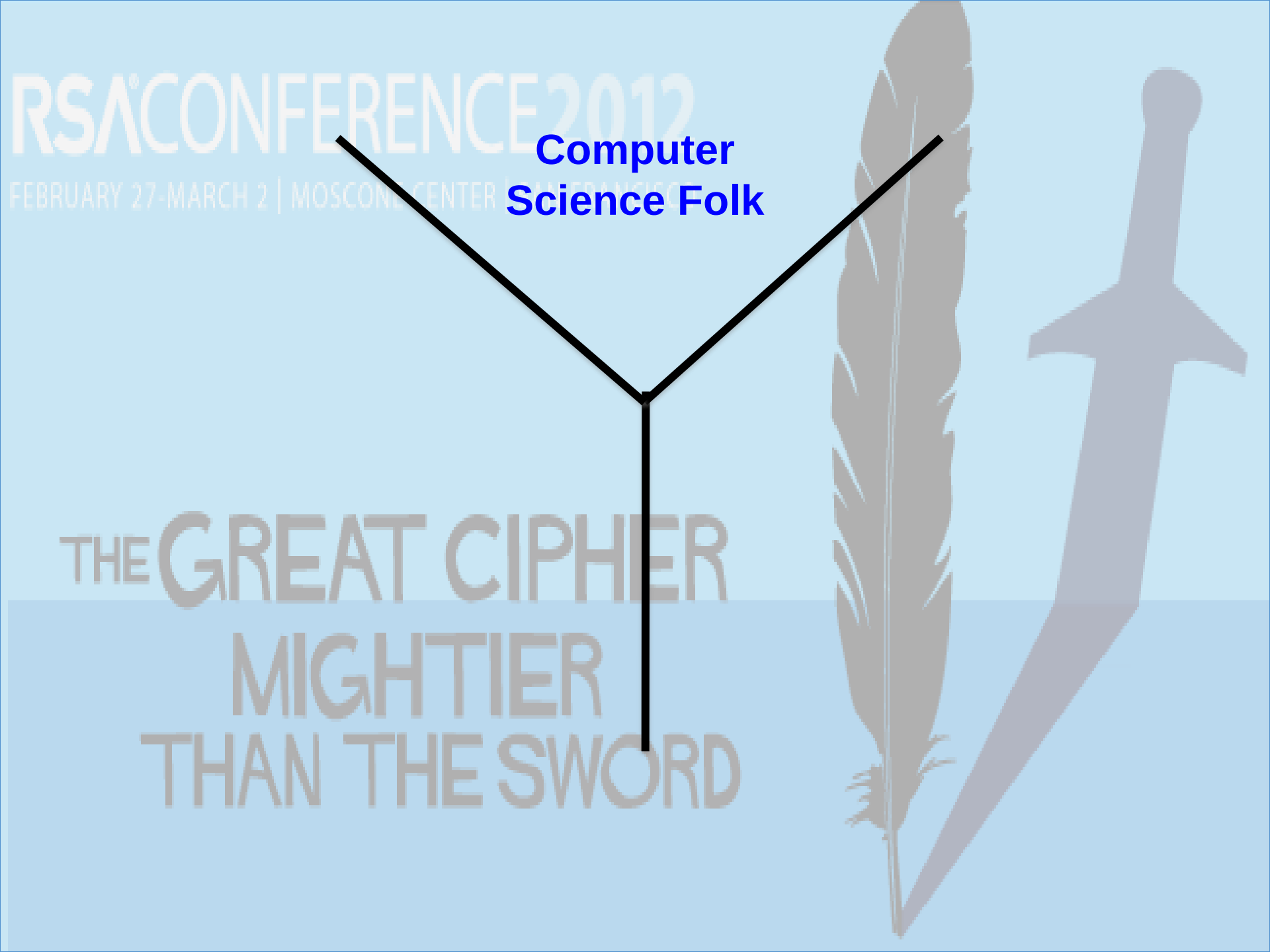

People
Capability
Technology
Information

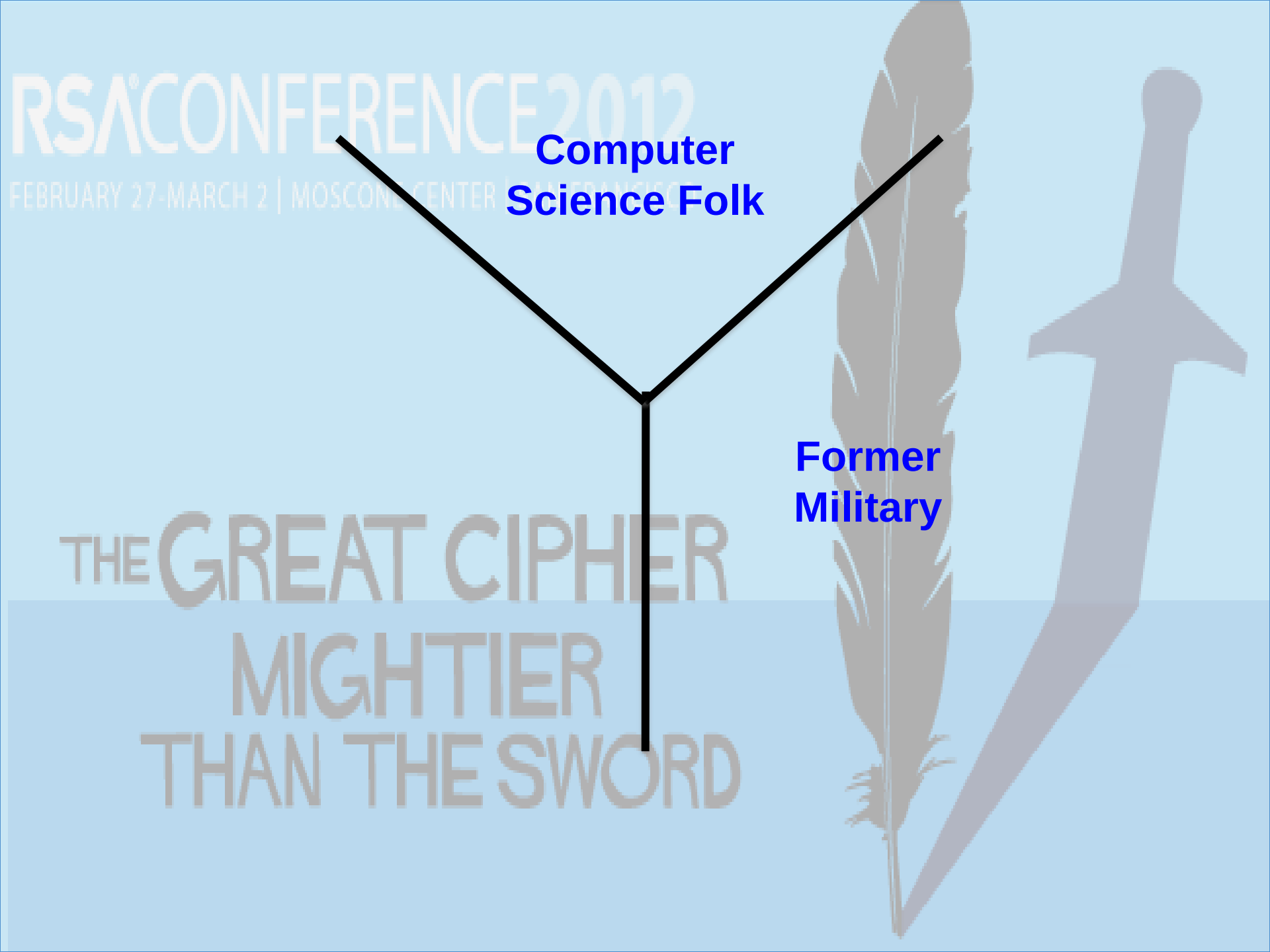
- *“Who should staff this theoretical team them?”*

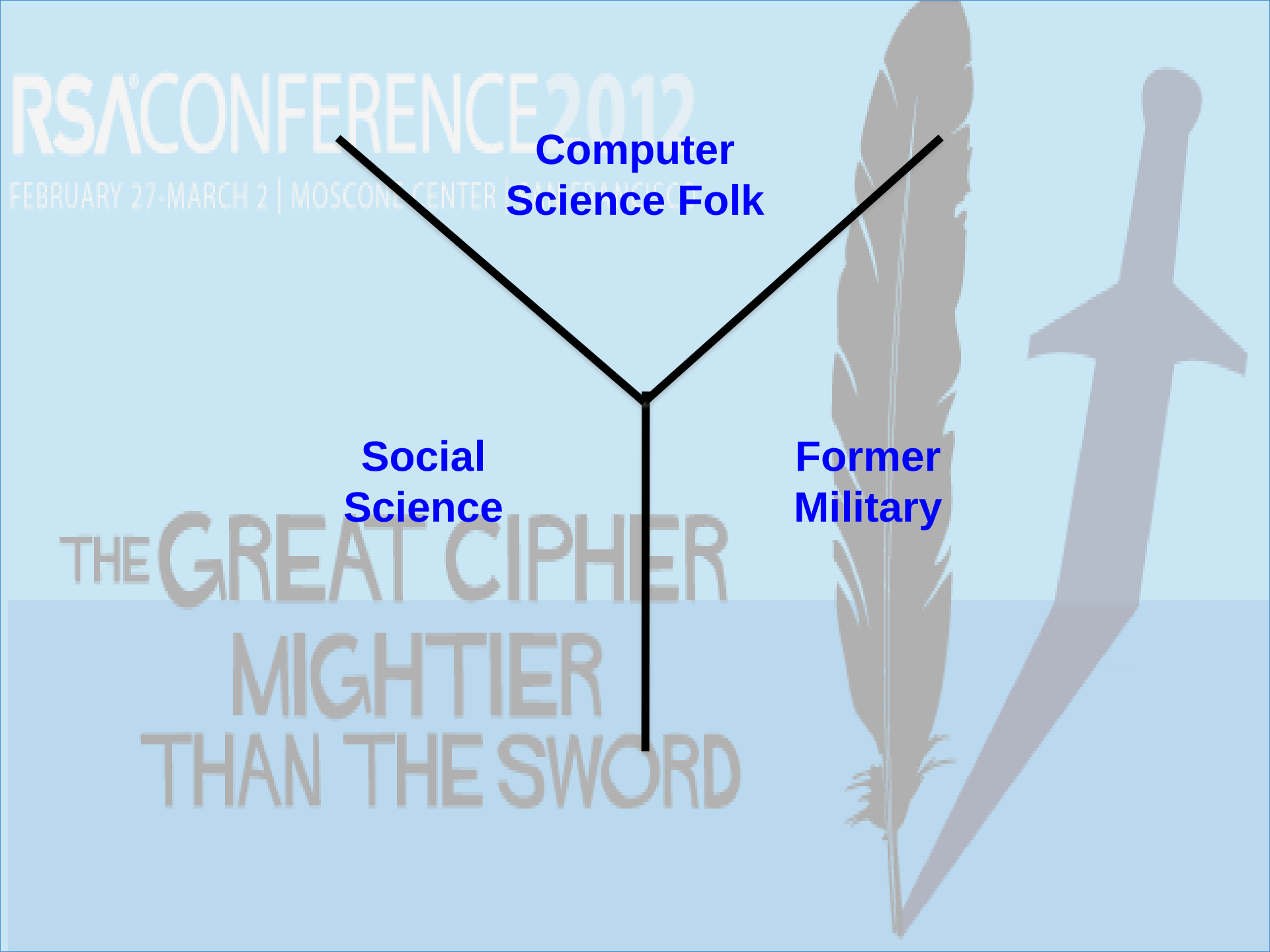
RSA CONFERENCE 2012

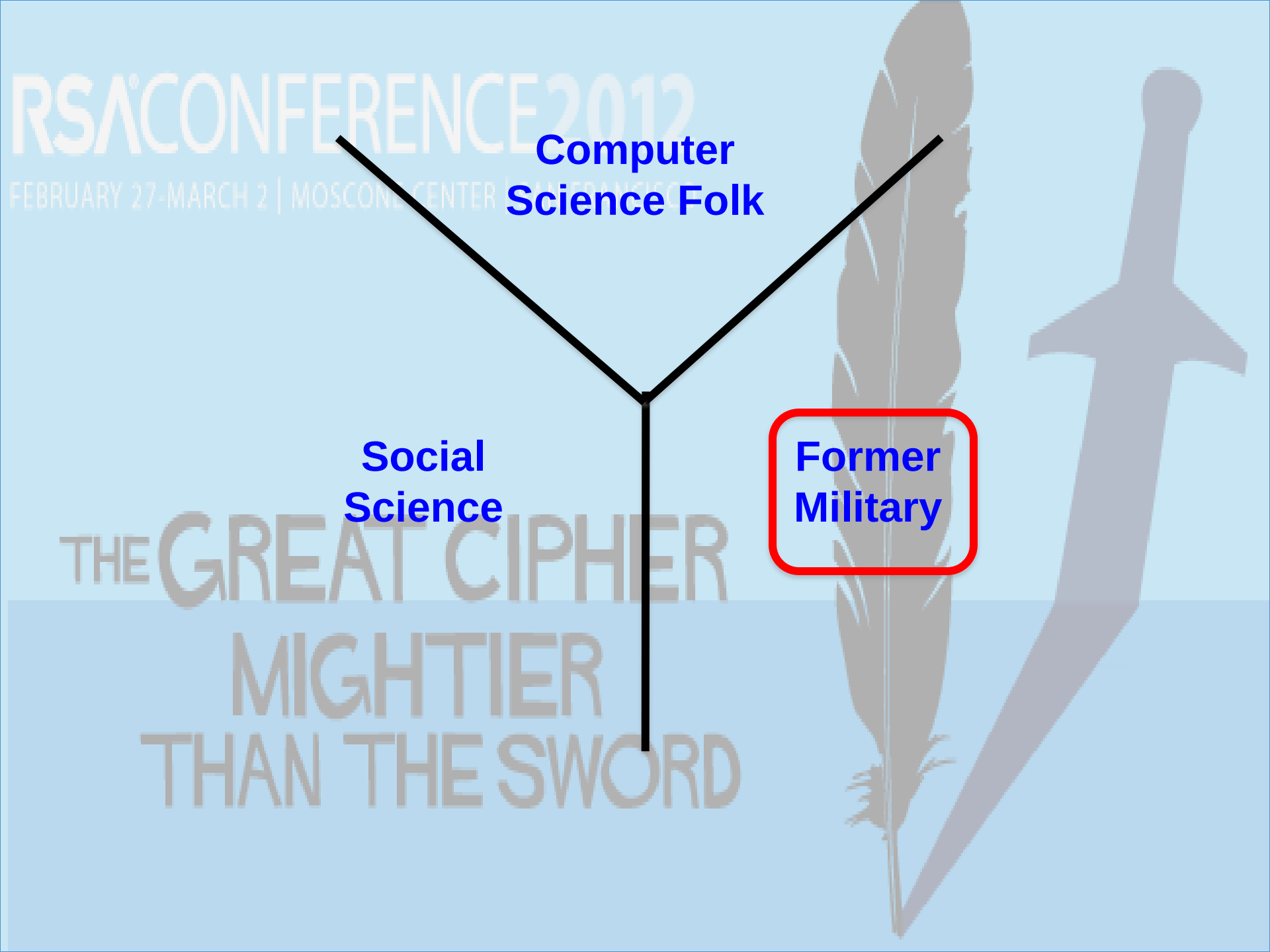
FEBRUARY 27-MARCH 2 | MOSCONE CENTER | SAN FRANCISCO

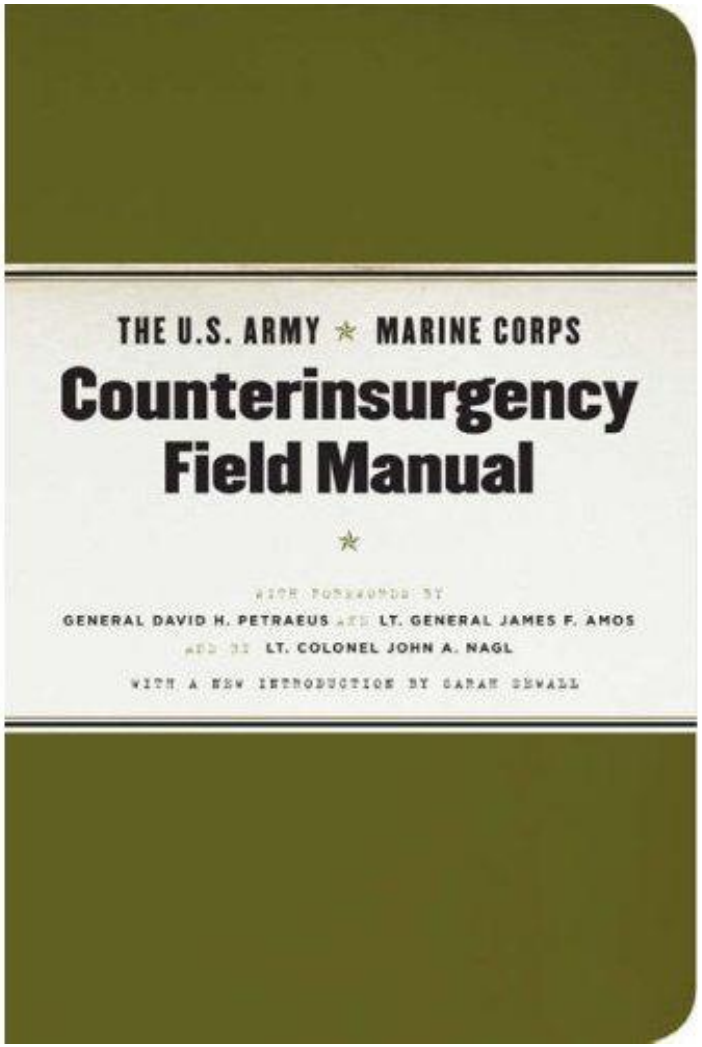
THE GREAT CIPHER MIGHTIER THAN THE SWORD


RSA CONFERENCE 2012
FEBRUARY 27-MARCH 2 | MOSCONE CENTER
Computer
Science Folk
THE GREAT CIPHER
MIGHTIER
THAN THE SWORD


Computer
Science Folk
Former
Military


Computer
Science Folk
Social
Science
Former
Military


Computer
Science Folk
Social
Science
Former
Military



Counter Insurgency (COIN)

- Battle for hearts and minds
- Human Terrain Analysis

ANONYMOUS VS SCIENTOLOGY

Search

COMMUNITY | EVENTS | ANONYMOUS » | SCIENTOLOGY »

Why We Protest Scientology

Our Goals

Initiatives

Anonymous vs Scientology
Discussions: 33,383 Messages: 992,508
Sub-Forums: 63
Latest: WSB-TV: State investigates...
JohnnyRUClear, 47 minutes ago

Freedom of Information
Discussions: 2,082 Messages: 48,675 Sub-Forums: 18
Latest: Barrett Brown: Threats To FBI...
Anonymous, 15 minutes ago

Iran
Discussions: 8,221 Messages: 45,785 Sub-Forums: 18
Latest: Killing of captured Iranians...
Anonymous, Today at 1:15 AM

Occupy Wall Street
Discussions: 169 Messages: 10,056 Sub-Forums: 3
Latest: One way to piss the bank off
Anonymous, Yesterday at 10:46 PM

Events

Planning
Discussions: 718 Messages: 8,651
Latest: [Oct 13, 2012] Chicago...
Joe's Body Thetans, Yesterday at 11:21 PM

Follow Up
Discussions: 155 Messages: 4,020
Latest: Sept. 29th Düsseldorf...
MOOG, Friday at 12:47 PM

Cross Initiative Resources

Production Studio
Discussions: 163 Messages: 3,631
Latest: Wikileaks Partnership to End...
AgentsOfTheFree, Friday at 11:11 PM

How To
Latest: Internet Explorer 9 fucking...

Donate

$160.00 Raised so far
$500.00 Monthly goal
32%

Donate

Top Donations

Guest
$200.00

Anonymous
$100.00


anonymouschanology
$100.00

Staff Online Now




Members Online Now

Title	Start Date	Replies	Views	Last Message ↓
[Oct 13, 2012] Chicago Scientology protest for October (Chicago, USA) Strong Strength, Sep 5, 2012		Replies: 31 Views: 628		Joe's Body Thetans Yesterday at 11:21 PM
[Nov 5, 2012] @OpVendetta2012 - 5th of November - London (Trafalgar square) dcht-ID, Jul 22, 2012		Replies: 35 Views: 1,345		Joe's Body Thetans Yesterday at 6:58 AM
[Oct 26, 2012] Enemies of the State: Solidarity for Bradley Manning, Julian... (New York, NY) anonymous2601, Friday at 4:01 PM		Replies: 3 Views: 95		anonymous612 Friday at 9:25 PM
[Oct 11, 2012] LONG CAT IS LONG (Groningen, Groningen) KittyKatSpanker, Sep 12, 2012		Replies: 14 Views: 628		Anonymous Friday at 9:13 AM
[Oct 20, 2012] Europaweiter Protesttag gegen INDECT Berlin (Berlin) Stiffmaster, Sep 13, 2012		Replies: 3 Views: 276		14198764829477292 Friday at 6:48 AM
[Nov 5, 2012] PROTEST FOR PEOPLE FROM SOUTH AUSTRALIA (SA) Tyain, Tuesday at 7:33 AM		Replies: 9 Views: 165		Anonymous Thursday at 3:37 AM
[Nov 1, 2012] OPERATION: BE EPIC (UNITED STATES) WExARExANONYMOUS, Sep 17, 2012		Replies: 7 Views: 823		Anonymous Wednesday at 2:01 AM
[Oct 20, 2012] Sponteneous Congregation of Disgruntled Laborers (New York NY) conatus, Sep 28, 2012		Replies: 3 Views: 149		another123 Sep 29, 2012
[Oct 6, 2012] Anonymous vs Scientology Rally (Dublin, Ireland) Nataku, Sep 26, 2012		Replies: 0 Views: 300		Nataku Sep 26, 2012
[Sep 22, 2012] Scientology Festival of FLUNK (San Fagcisco, CA) skeptic2girl, Sep 10, 2012		Replies: 5 Views: 199		Anonymous Sep 19, 2012
[Sep 22, 2012] Anonymous vs Scientology Rally (Dublin, Ireland) Nataku, Sep 9, 2012		Replies: 2 Views: 256		Anonymous Sep 17, 2012
[Sep 12, 2012] Vow of Silence (All Public Locations.) liveANONYMOUS, Sep 12, 2012		Replies: 2 Views: 112		liveANONYMOUS Sep 12, 2012

Anonymous
Member

It took 42 Minutes for your latest crap to be domed. Wonder how long this thread will take?

Betting windows are open!

Anonymous, Sep 26, 2012 #3 Reply

Mutante
Member

People are people? What about clones?

Mutante, Sep 26, 2012 #4 Reply

Like x 1 List

Anonymous
Member

> Bud said: ↑
>
> *Speaking for oneself is hard these days.*
> *It's much easier to get one's thought through some demotivator that seems to be appropriate. at this time.*

OFF is the general direction in which I'd like you to fuck, Scientologist.

How's that for a non-demotivational demotivational?
Fucknut.

Anonymous, Sep 26, 2012 #5 Reply

Anonymous
Member

Y'all niggaz postin' in a TROLL thread

LOL

Anonymous, Sep 26, 2012 #6 Reply

> Anonymous said: ↑
>
> *Y'all niggaz postin' in a ~~TROLL~~ future Dome thread*
>
> *LOL*

OpInfoStorm: Help us translate Anon and WWP flyers into Spanish!

Discussion in 'Production Studio' started by LastOneStanding, Aug 30, 2011.

LastOneStanding
Member

Most of the graphic content related to Anonymous is written in English. It's time to join forces and help make the Spanish forum as formidable as the English one. Lets put our designs in this thread, do some critical work to improve them and build a collection of graphic materials of high quality advertising, as only Anonymous can do it!

IF you need help with translations feel free to PM me or silly433.

We appreciate your halp

LastOneStanding, Aug 30, 2011 #1 Reply

Anonymou Synapse and Nishimori like this.

OpInfoStorm: Help us translate Anon and WWP flyers into Spanish!

Discussion in 'Production Studio' started by LastOneStanding, Aug 30, 2011.

LastOneStanding
Member

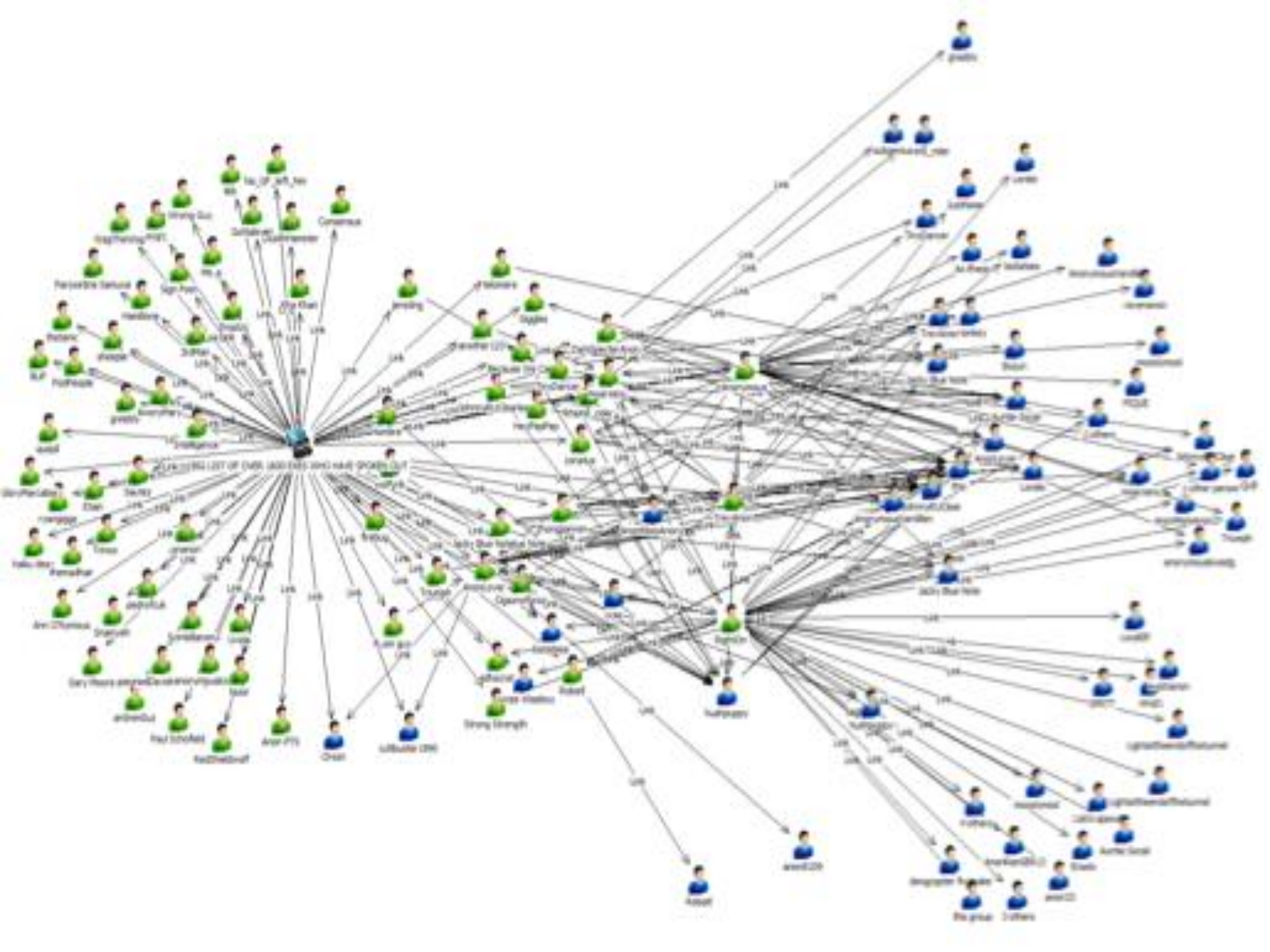
Most of the graphic content related to Anonymous is written in English. It's time to join forces and help make the Spanish forum as formidable as the English one. Lets put our designs in this thread, do some critical work to improve them and build a collection of graphic materials of high quality advertising, as only Anonymous can do it!

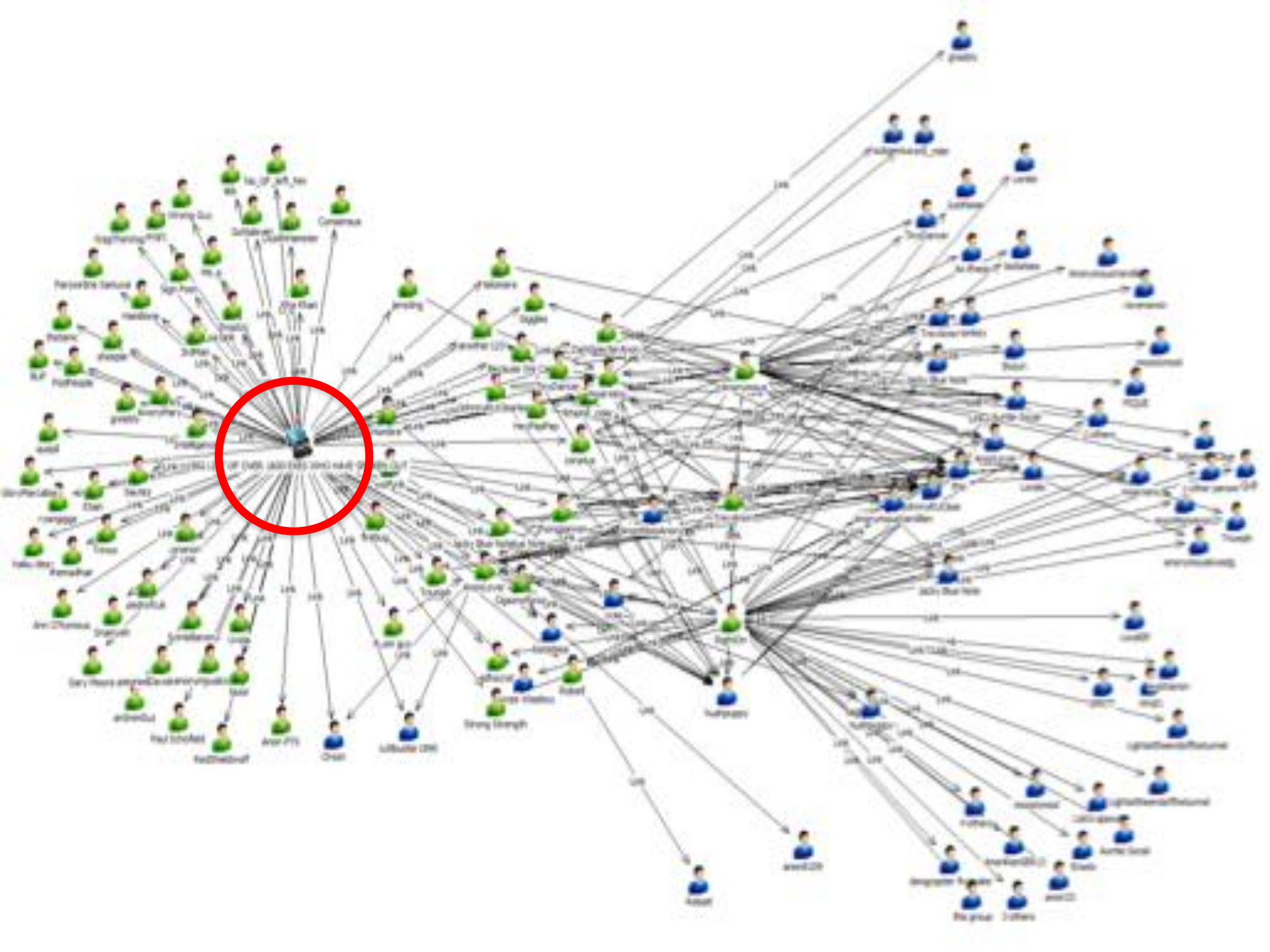
IF you need help with translations feel free to PM me or silly433.

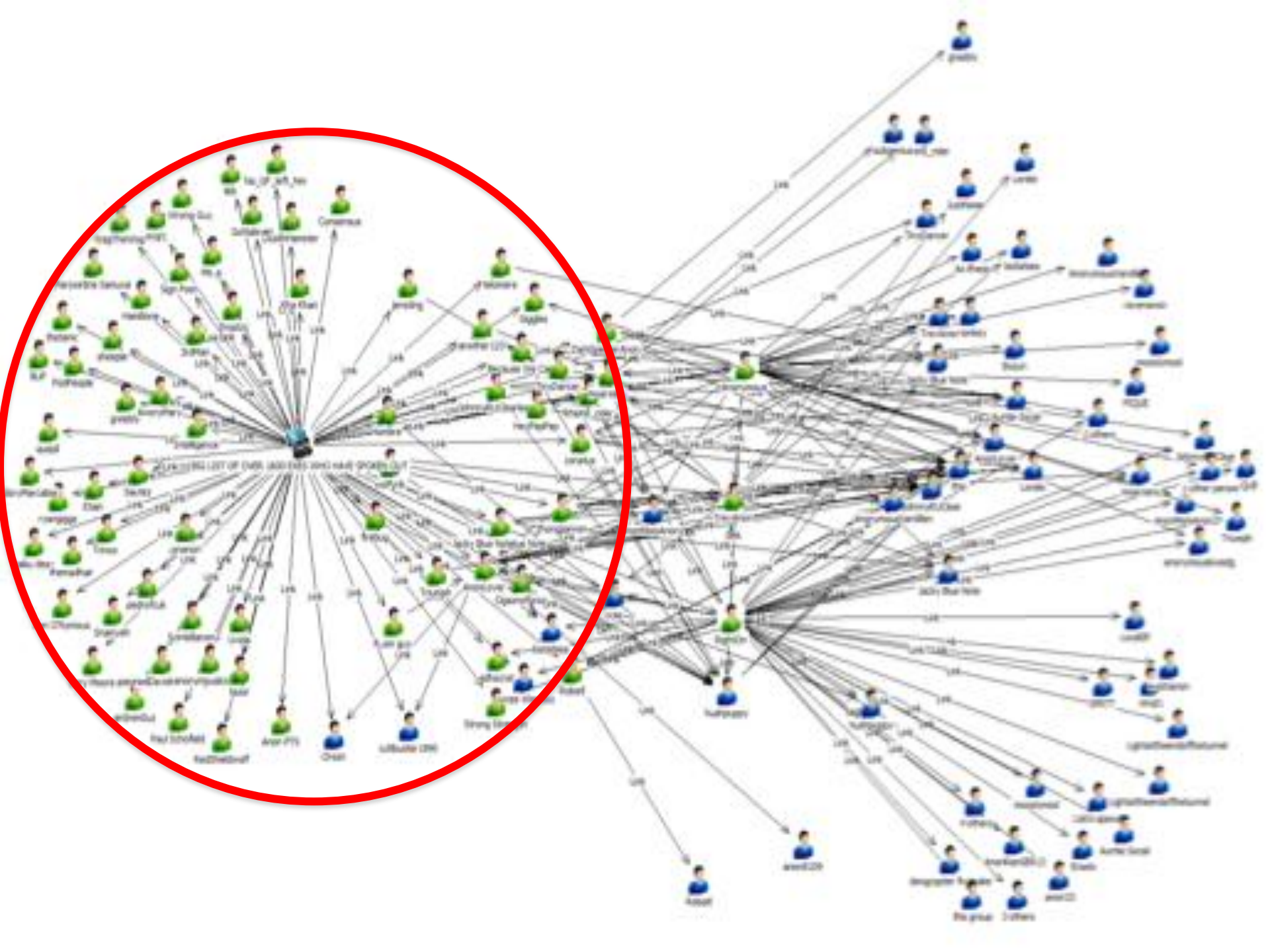
We appreciate your halp

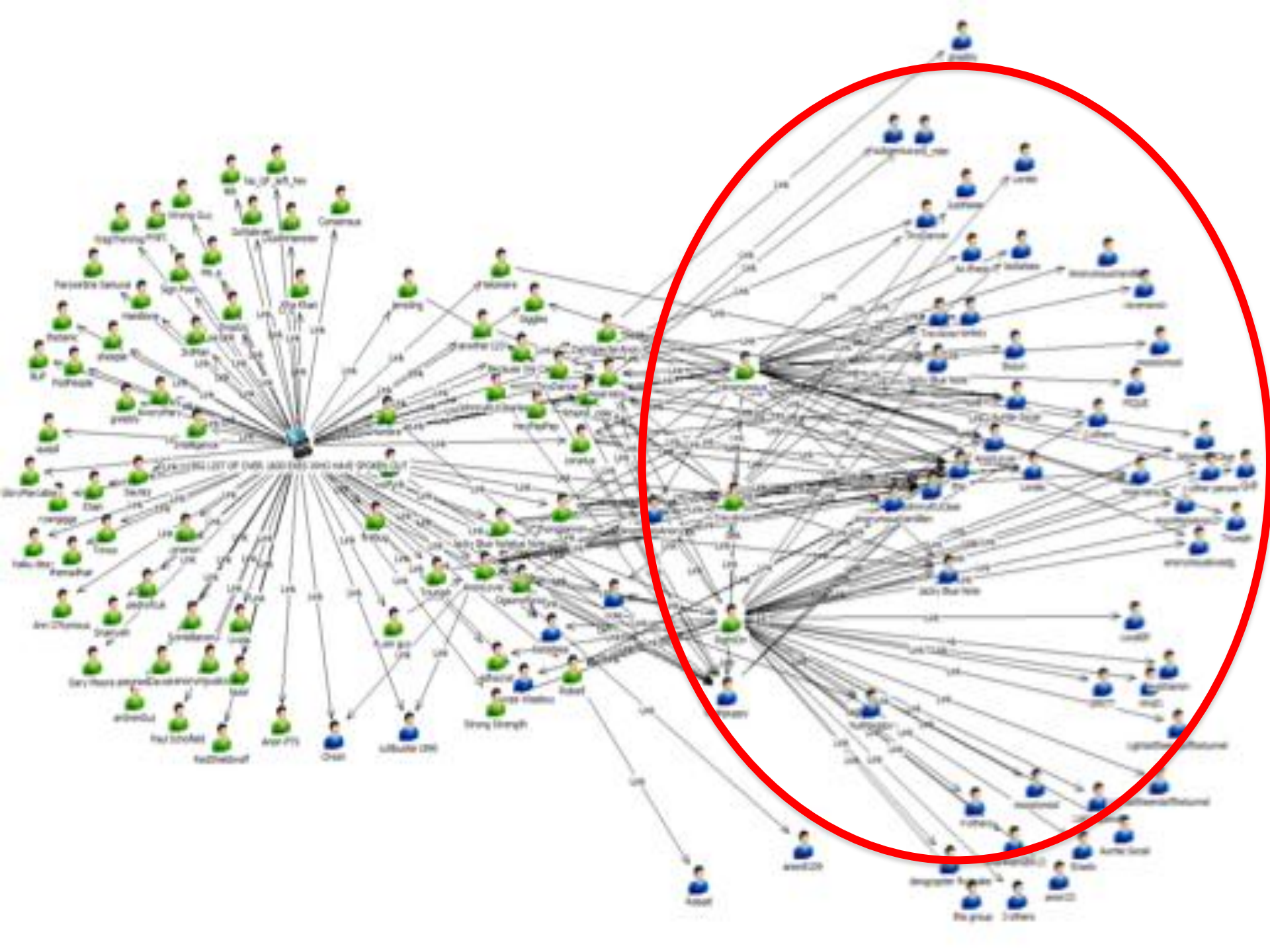
LastOneStanding, Aug 30, 2011 #1 Reply

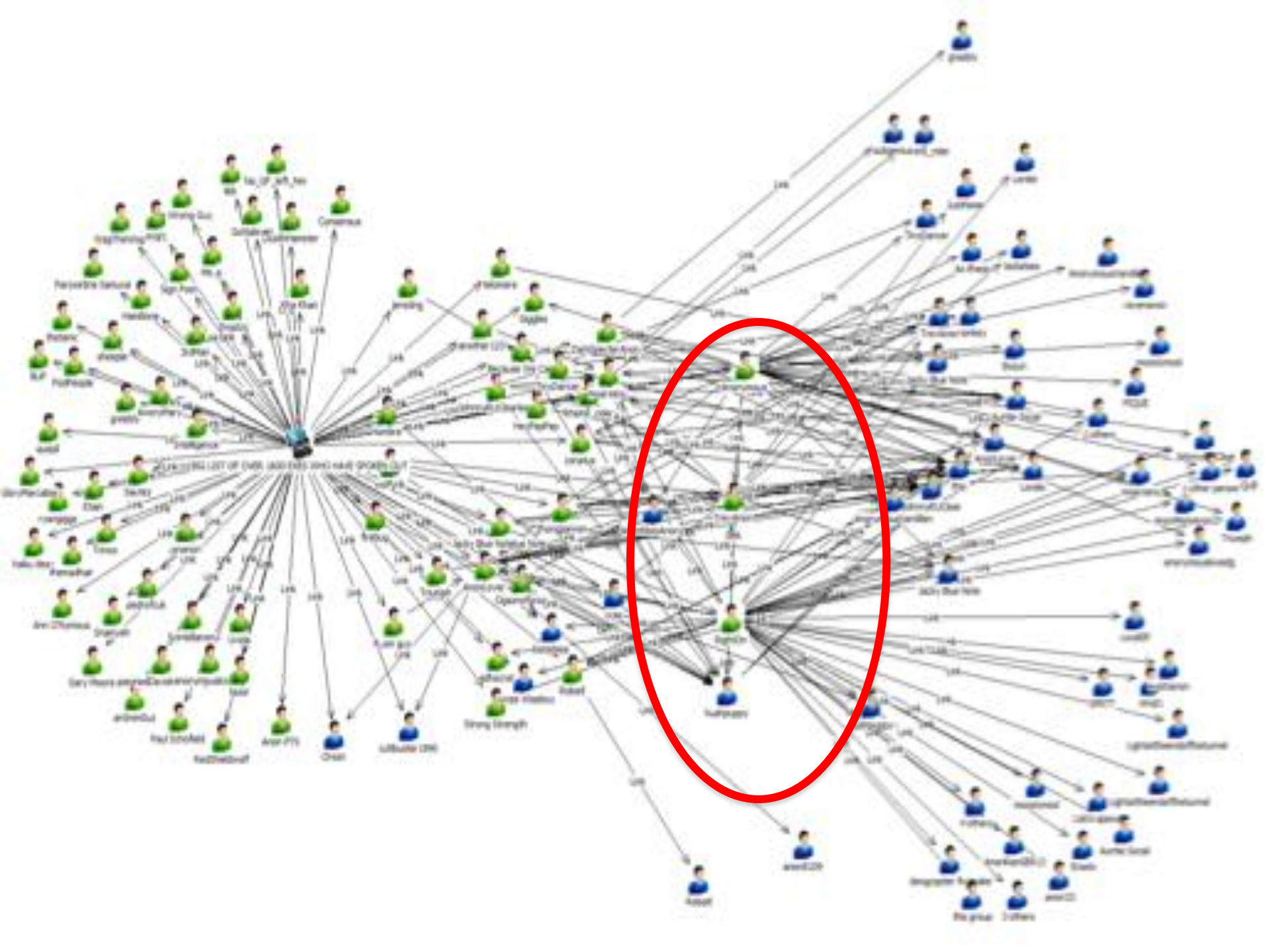
Anonymou Synapse and Nishimori like this.

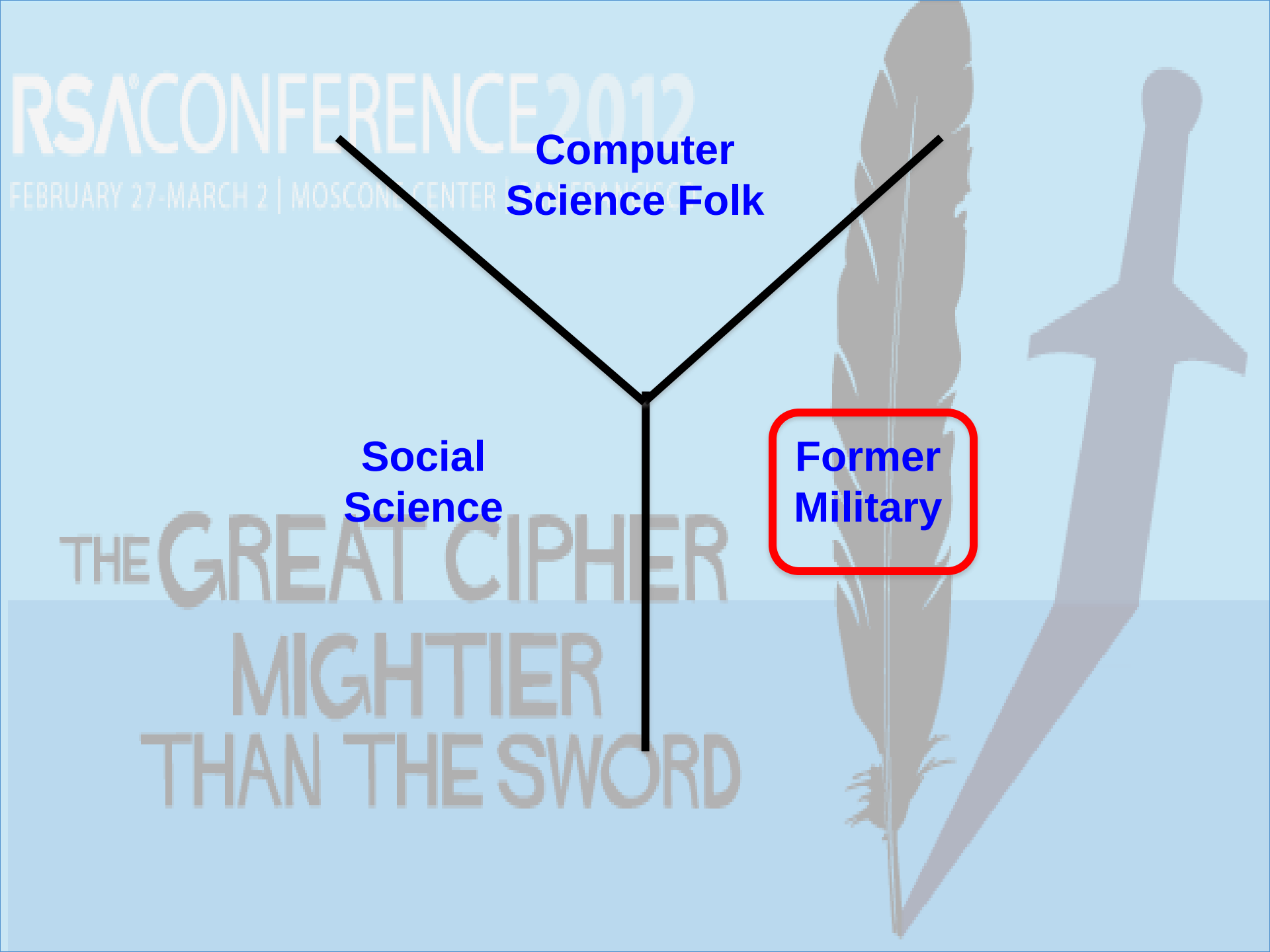


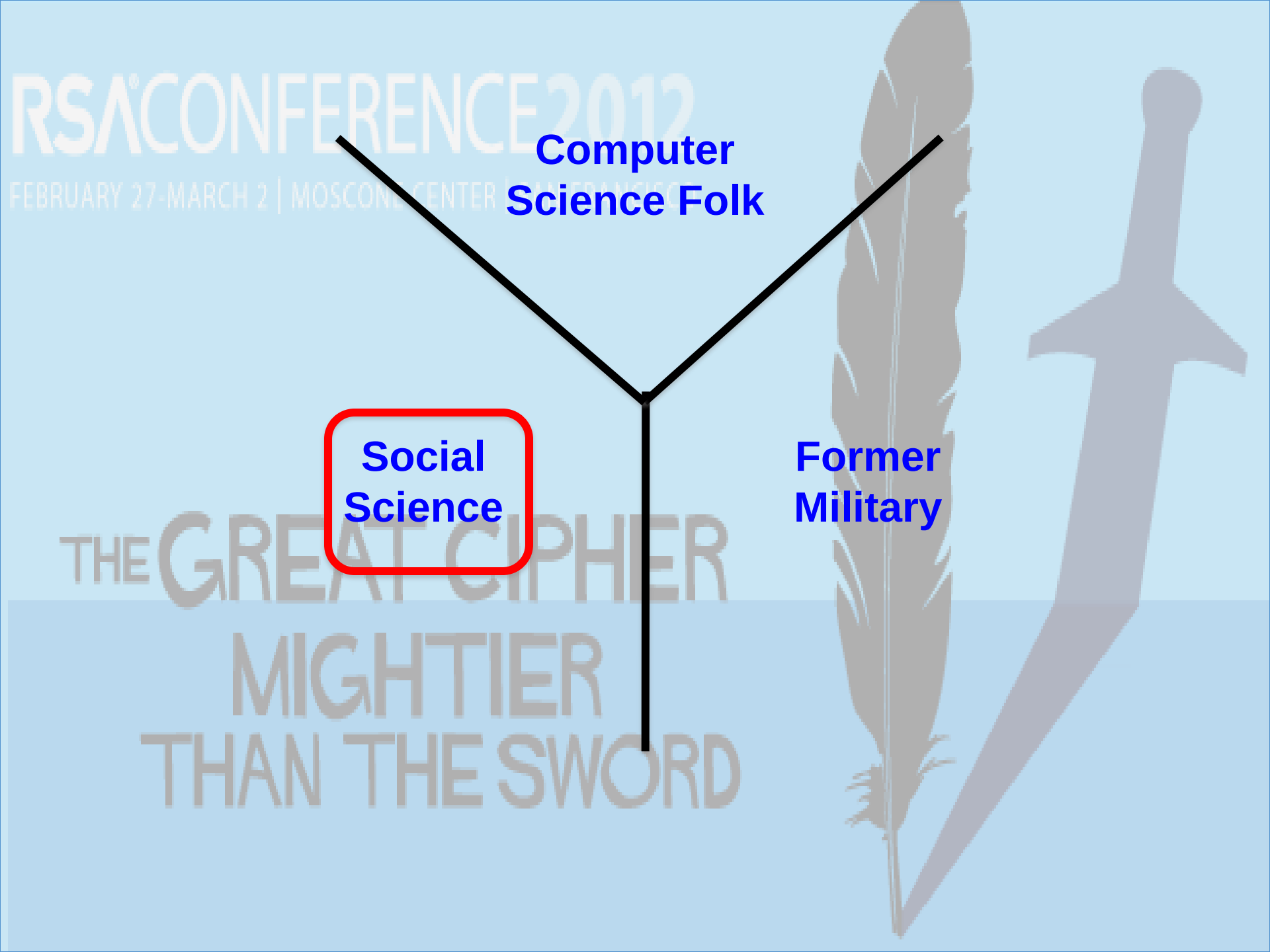


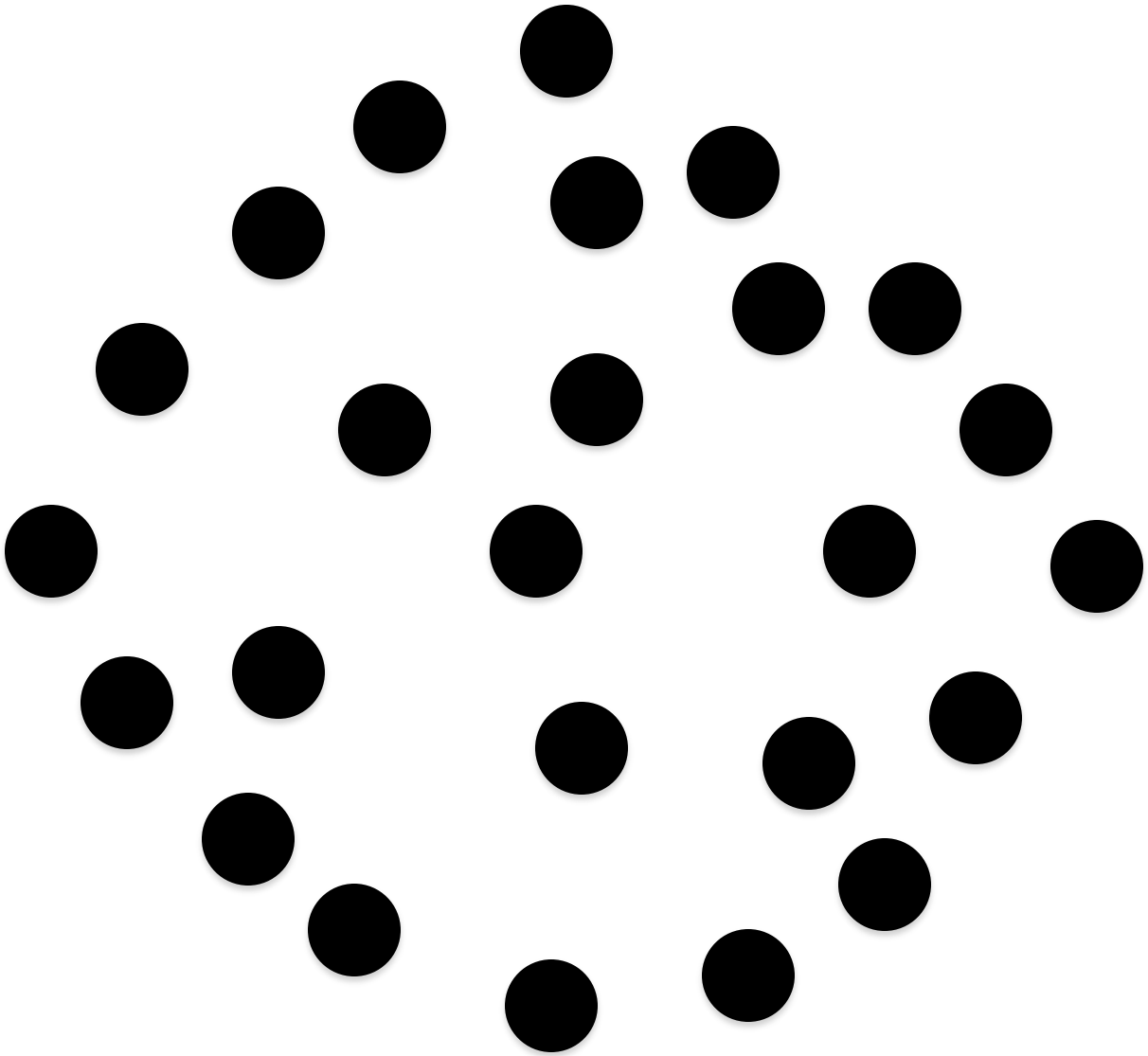


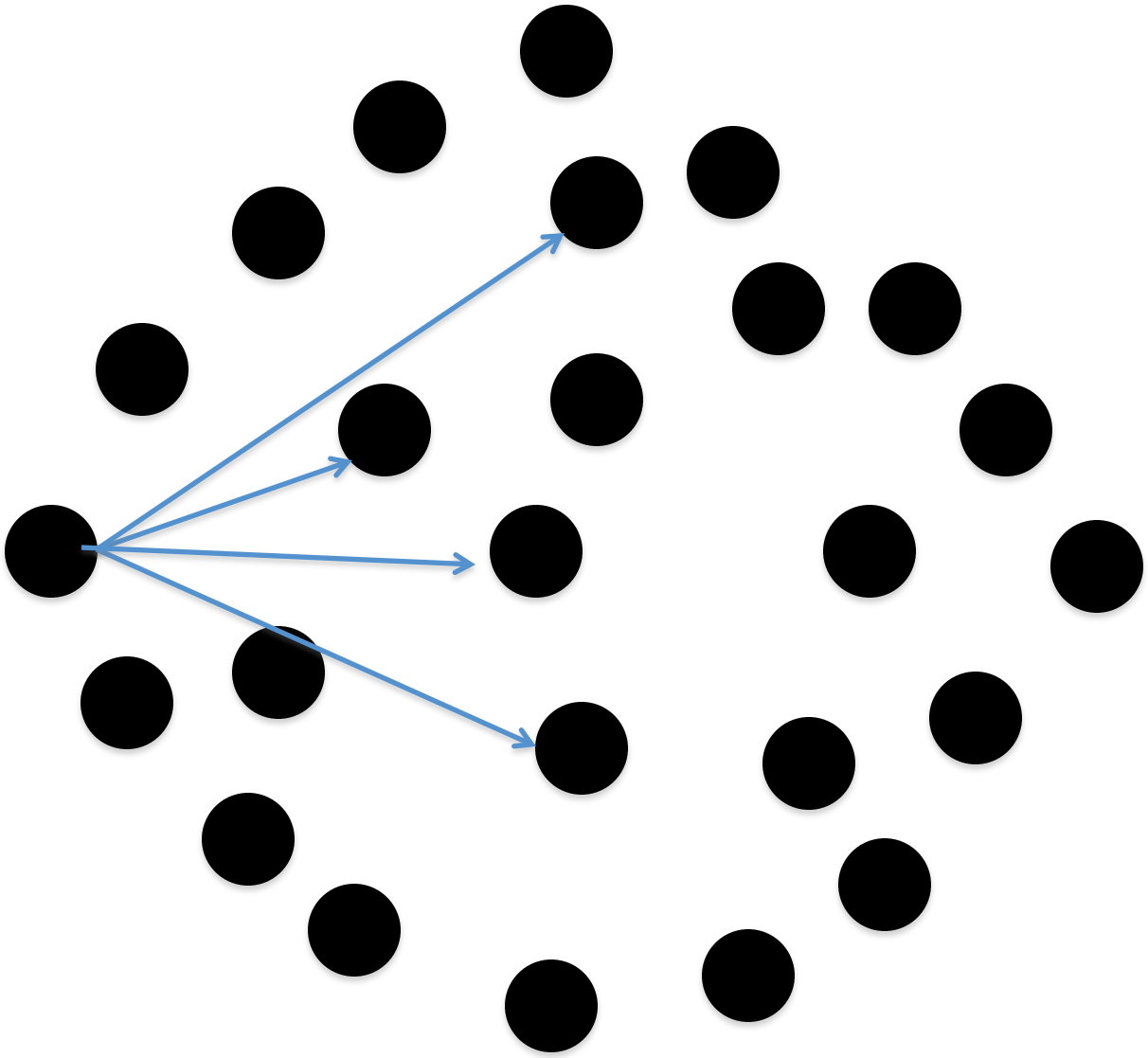





Computer
Science Folk
Social
Science
Former
Military

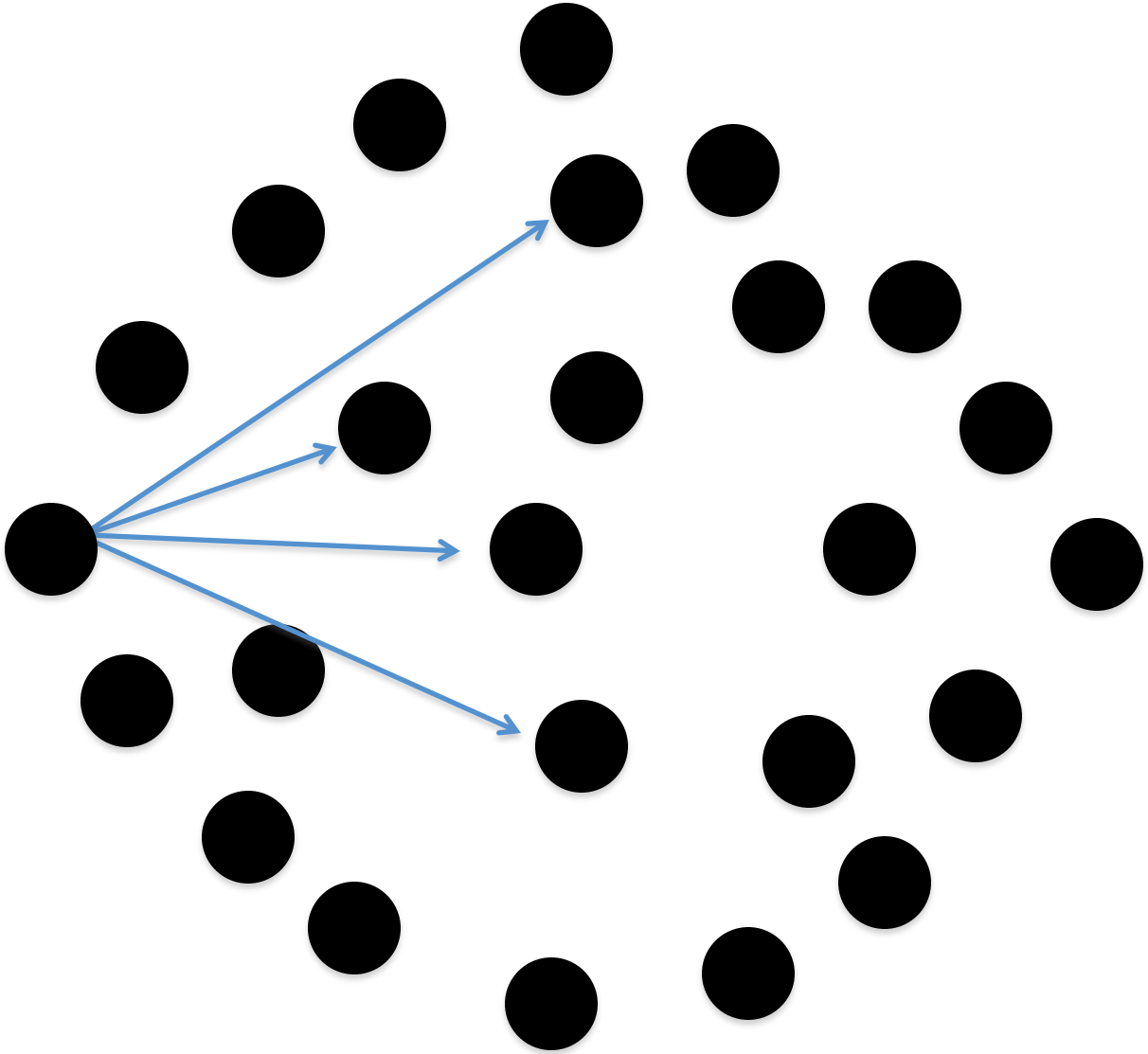

Computer
Science Folk
Social
Science
Former
Military



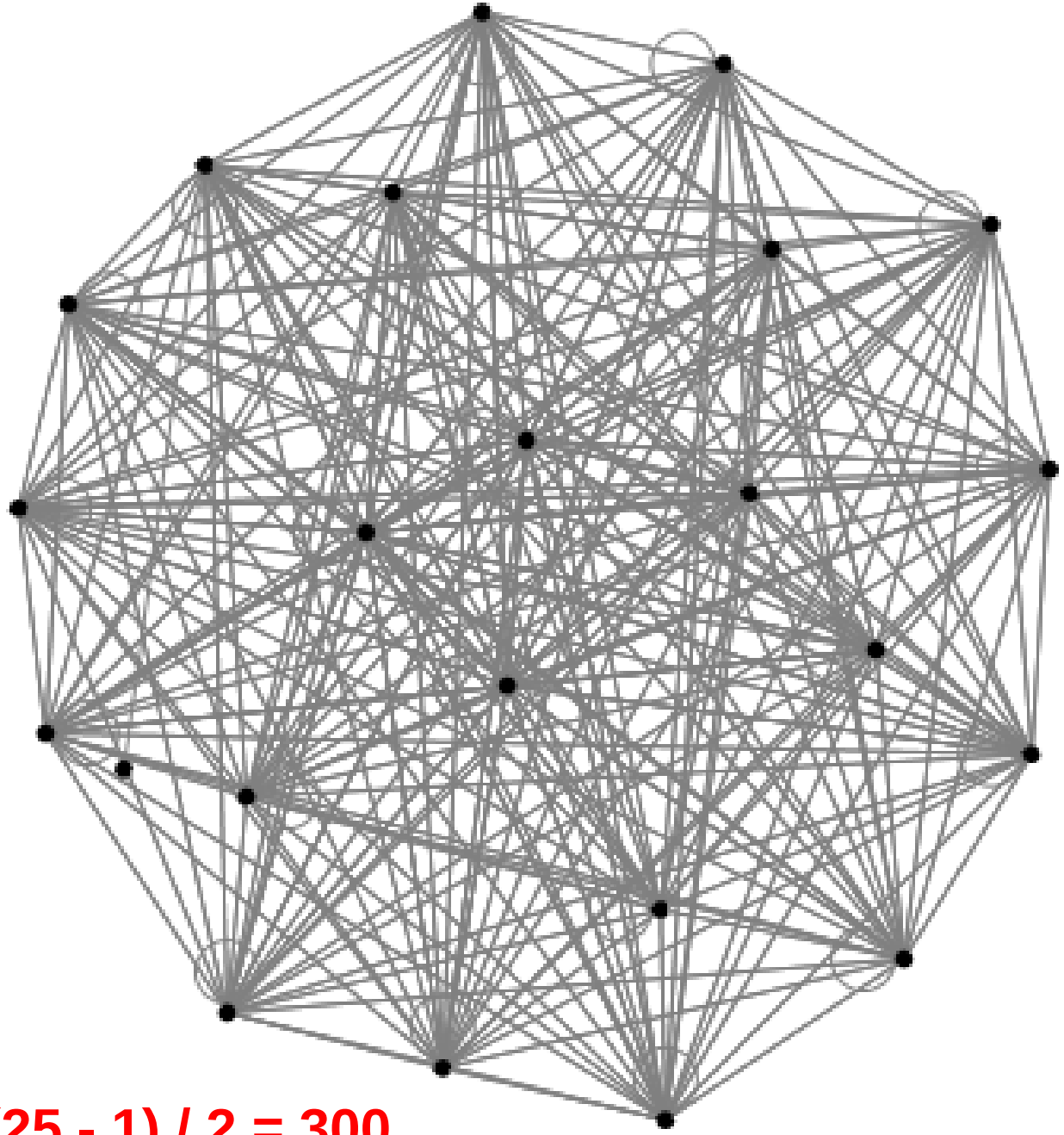


How many possible connections can be made within this group?

Clustering Coefficient



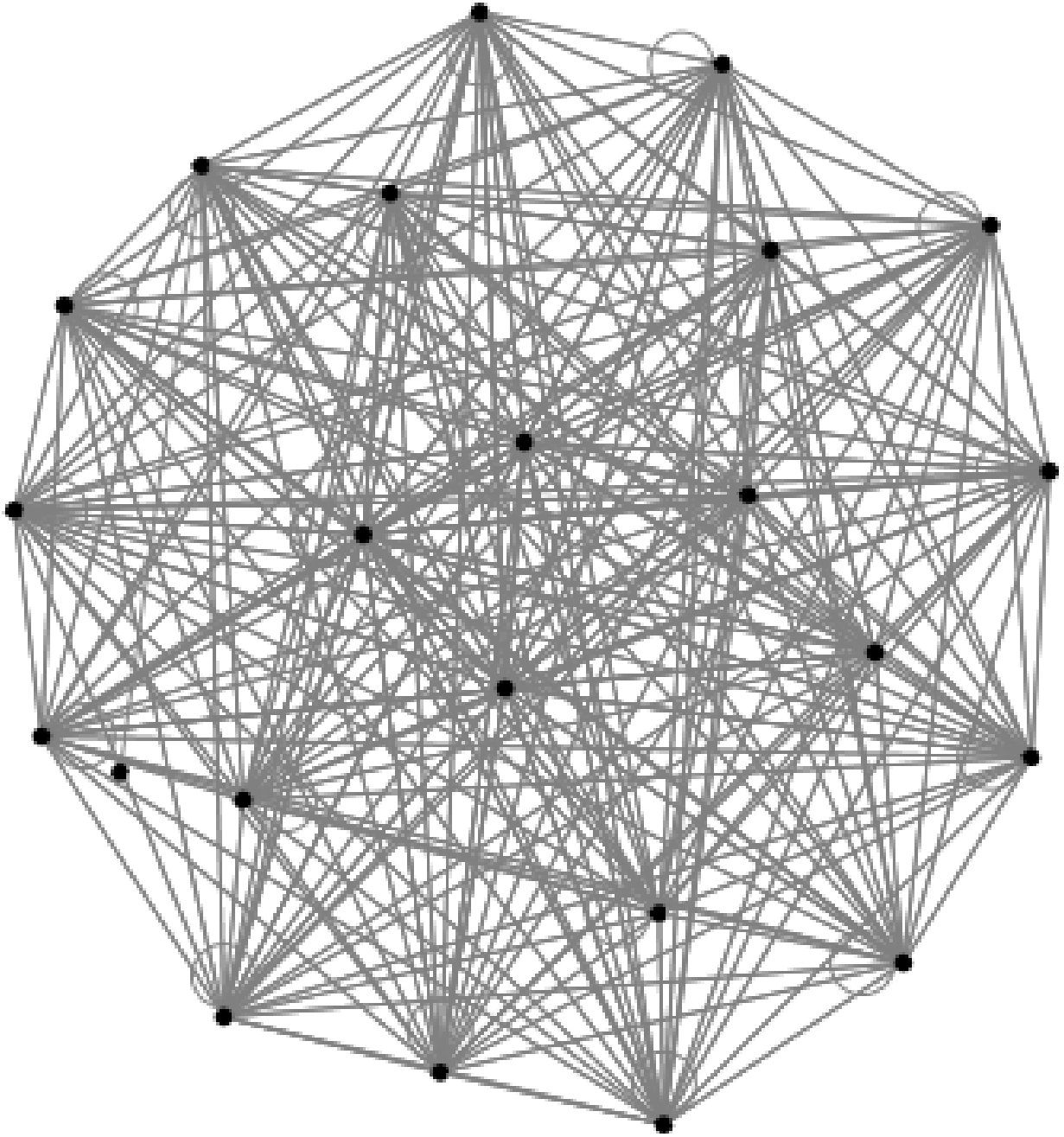
N * (N - 1) / 2

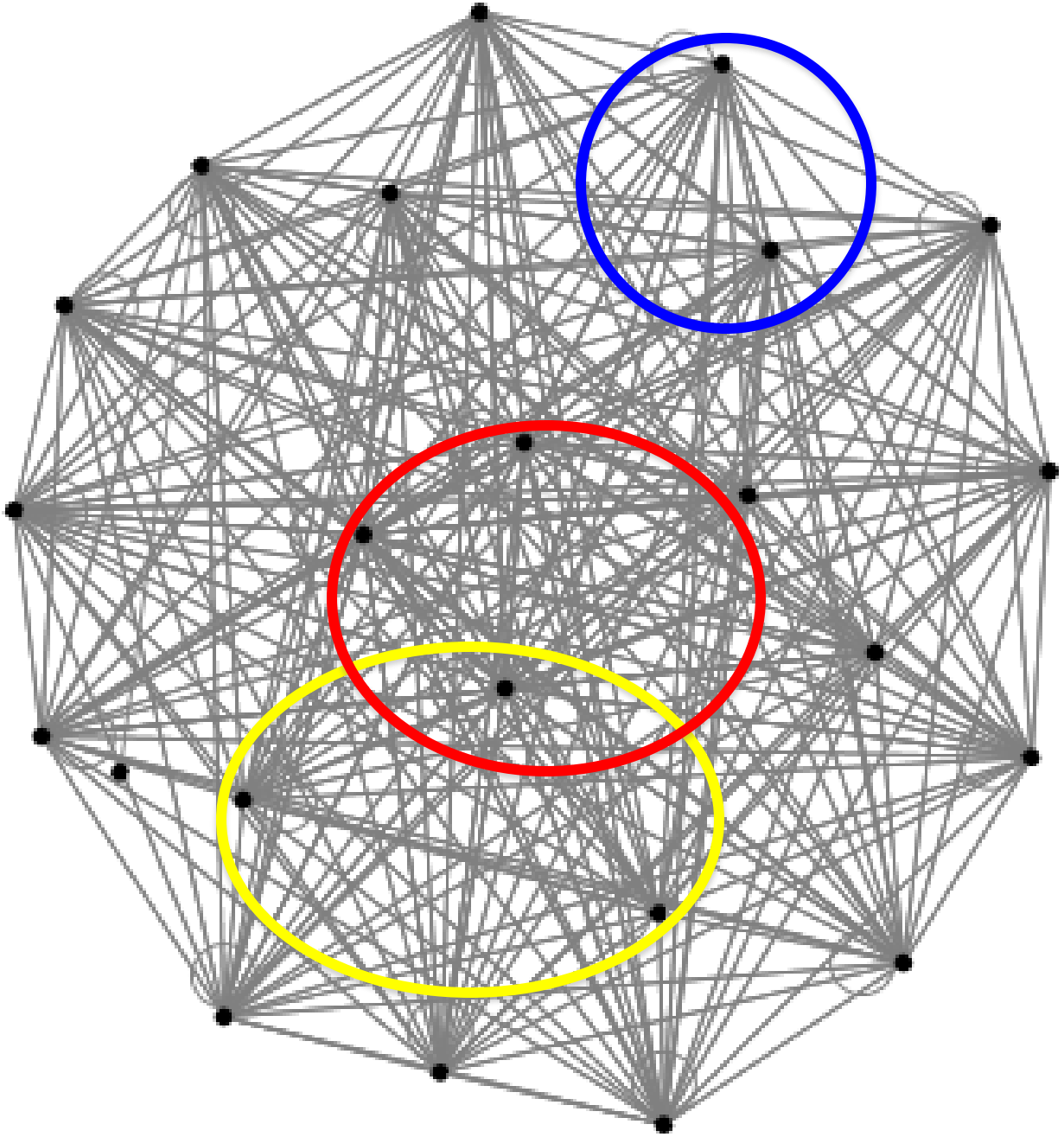


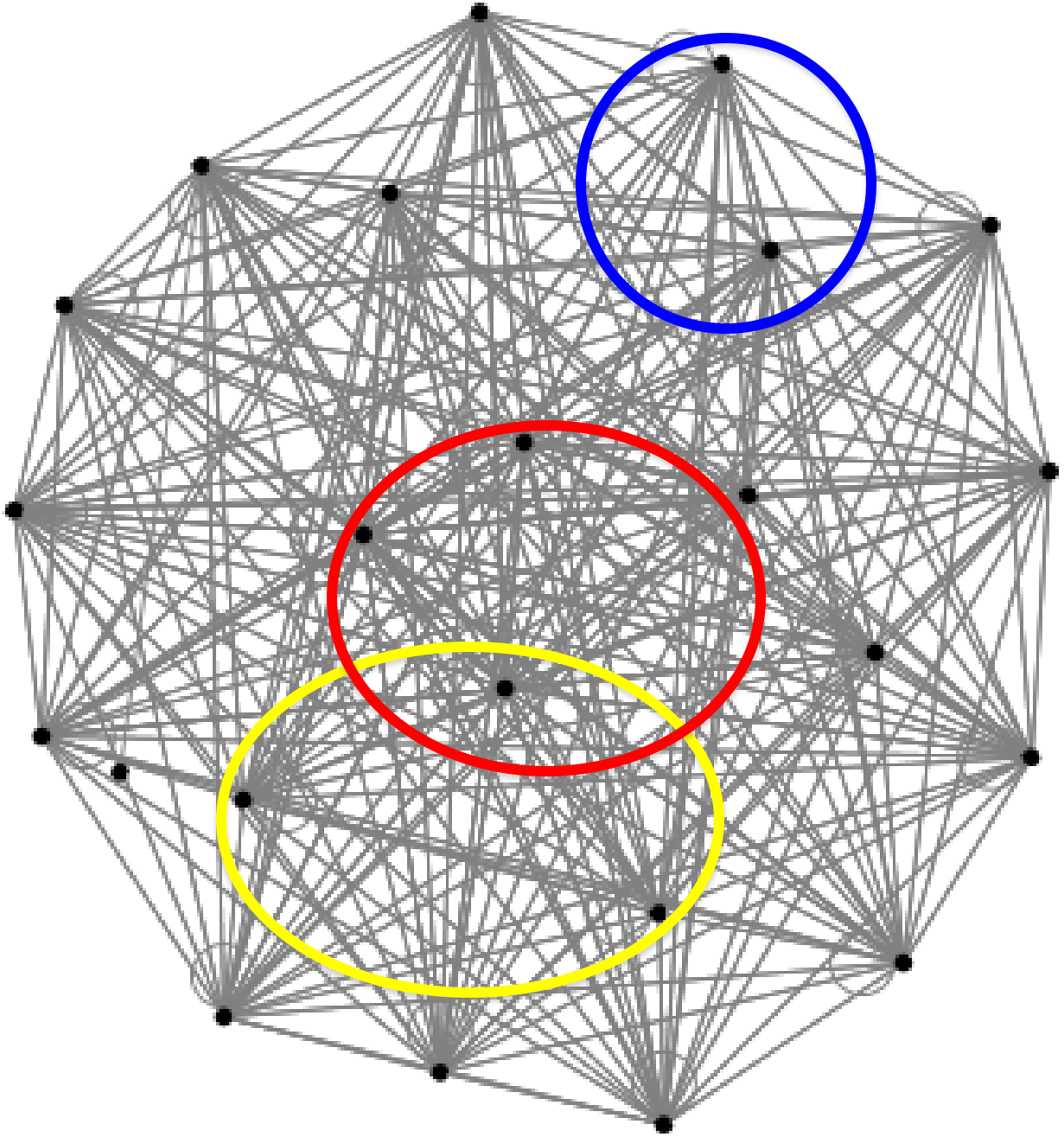
25 * (25 - 1) / 2 = 300

However…consider this

- John P. Reed
- the utility of large networks, particularly social networks, can scale exponentially with the size of the network.







33 Million possible combinations!!!!!!!!!

Home | AnonOps << | #anonleaks (19) | #anonsec (58) | #antisec (430) | #target (25) | #voice (68)

HACKERS UNITE AGAINST CORRUPTION ALL OVER THE WORLD! || READ: http://is.gd/8aoGqD || Got any info/leaks? /msg any SOP (&) in channel || http://thepiratebay.org/user/AntiSecu

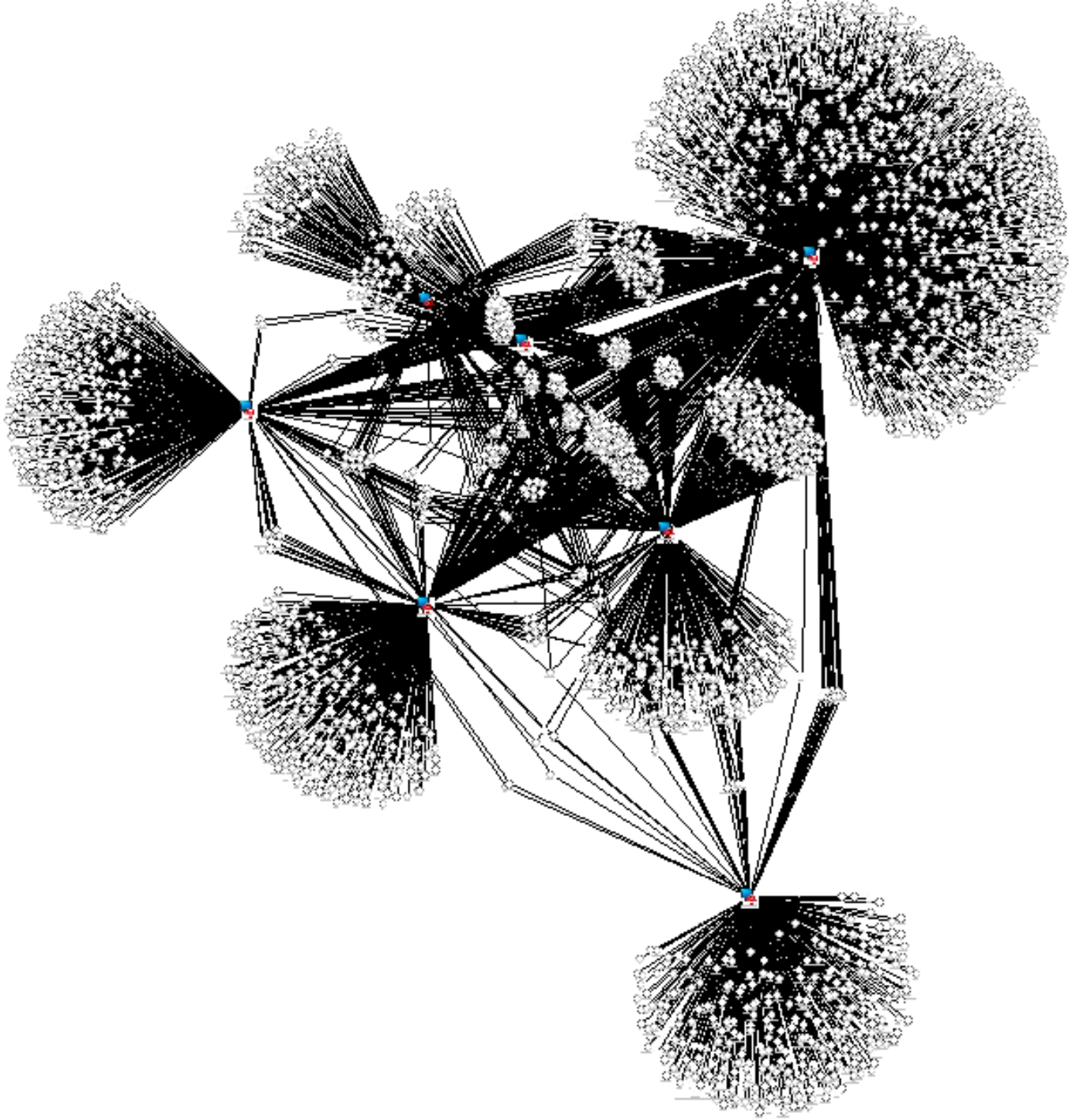
11:26	zerodivision	
11:26	Th3-5p3ctr3	Nothing worth doing is easily accomplished.
11:26	ti	
11:26	ti	this is true
11:26	anonArc	Th3-5p3ctr3, who said that ?
11:26	ti	not even fapping
11:26	Th3-5p3ctr3	DDoSing stuff is easy too, and you see what little that's accomplished besides a few kids getting v&
11:26	zerodivision	but no local stations.. I hope were talking CNN, BBC etc...
11:27	proSI	Brb
11:27	Th3-5p3ctr3	anonArc: Damned if I remember or I'd give them credit.
11:27	ti	it'd be cool to do stuff like captain midnight style
11:27	anonArc	lol
11:27		*** random quit (Connection closed)
11:27	ti	or the max headroom hack
11:27		*** proSI quit (Quit: used jmIrc)
11:27	anonArc	ti, YES
11:27	Th3-5p3ctr3	Besides, wouldn't be too hard with the right insider...
11:27	anonArc	they never found him you know
11:27	ti	lol yeah and he was totally nuts
11:27		*** dip quit (Connection closed)
11:28		*** BlacKHaT quit (Ping timeout: 121 seconds)

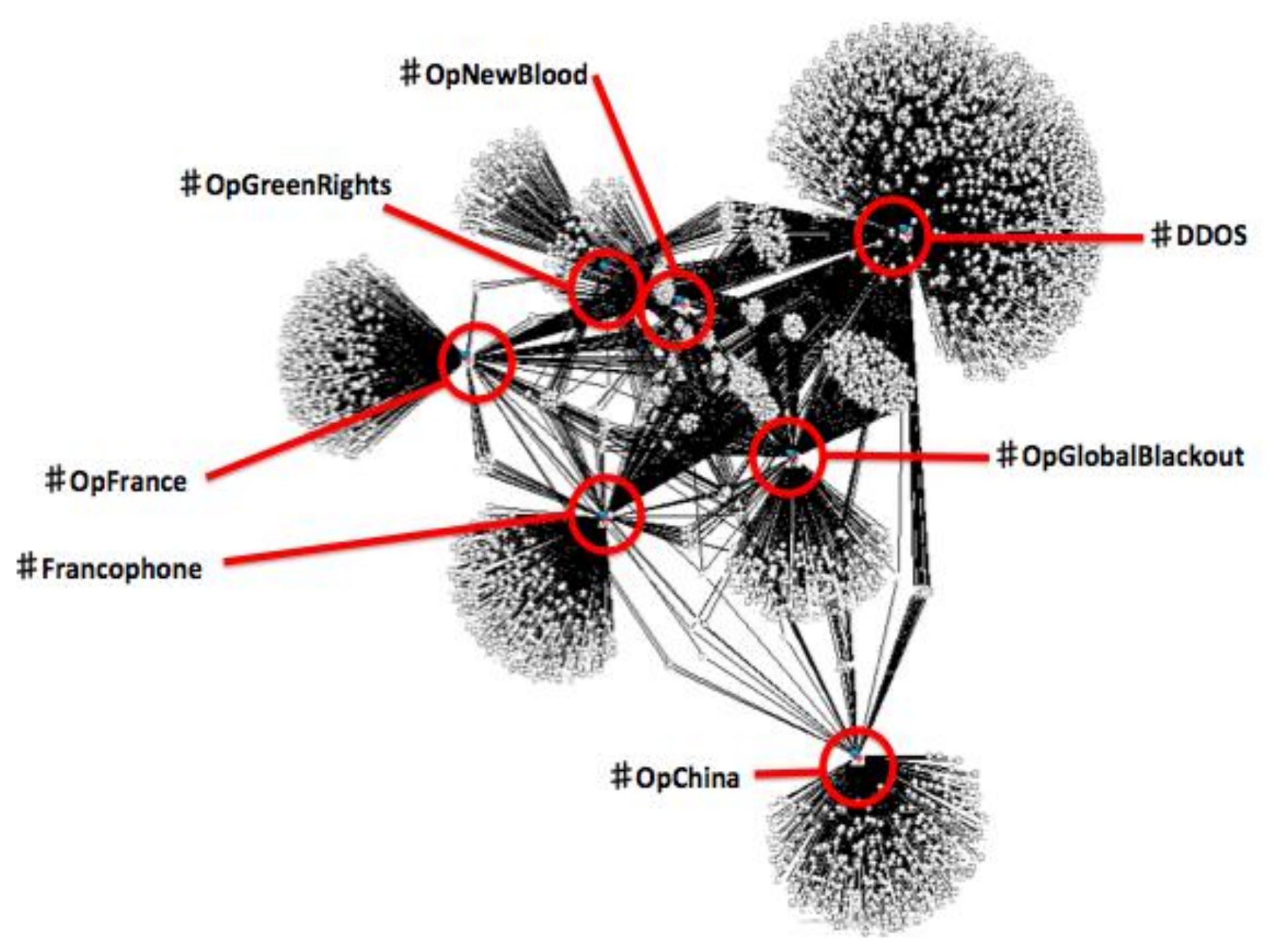
Chatting
InformationTerro
storm
Effexor
Troy
anonArc
Drefsab
Th3-5p3ctr3
ti
zerodivision

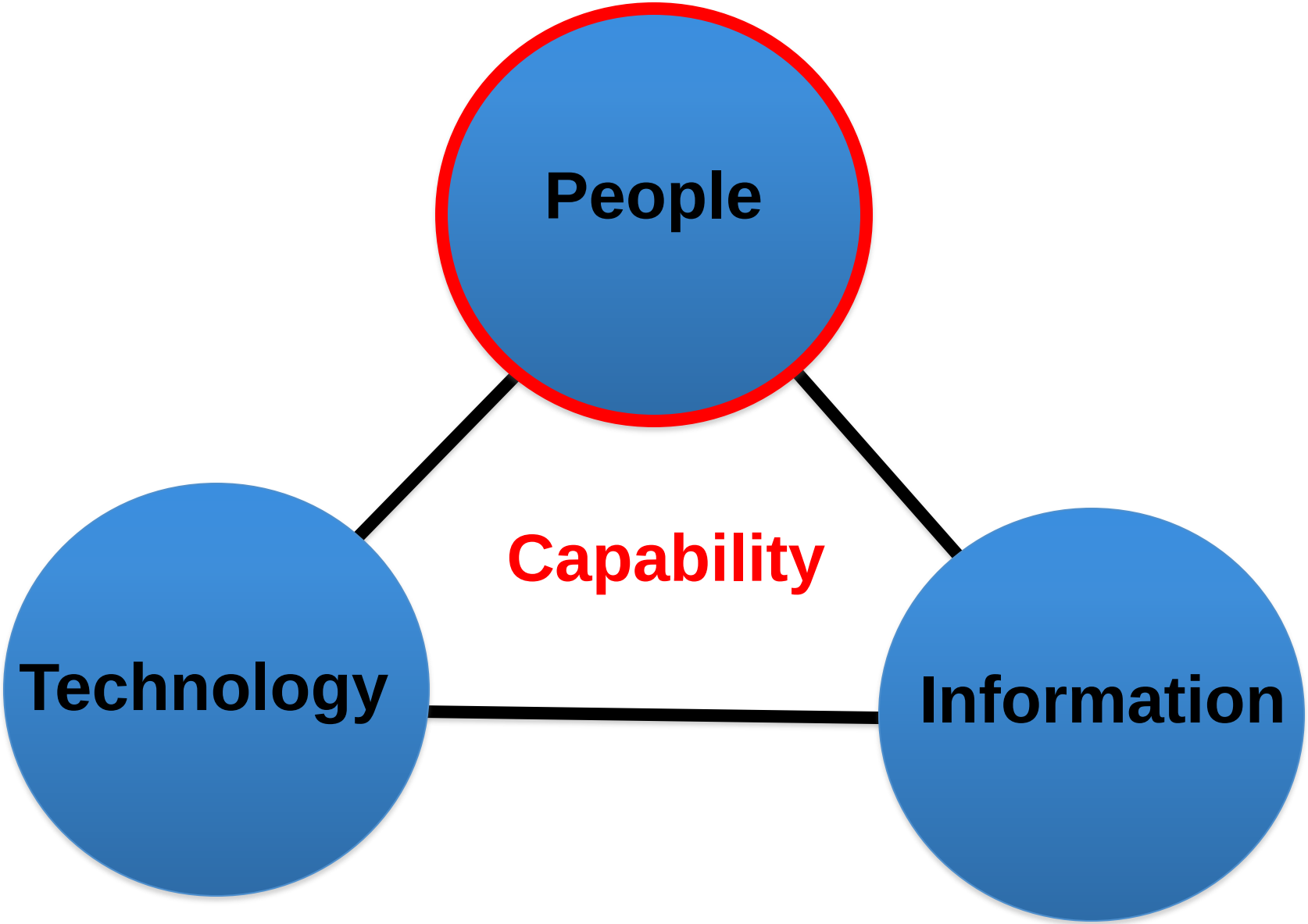
Idlers
marduk
Lulzboat
rum
Sabu
daboogieman
f[x]
GlomeX
jester
joepie91
p2a
shift
someloser
Fox
mr[a]
Nijaxor
selket

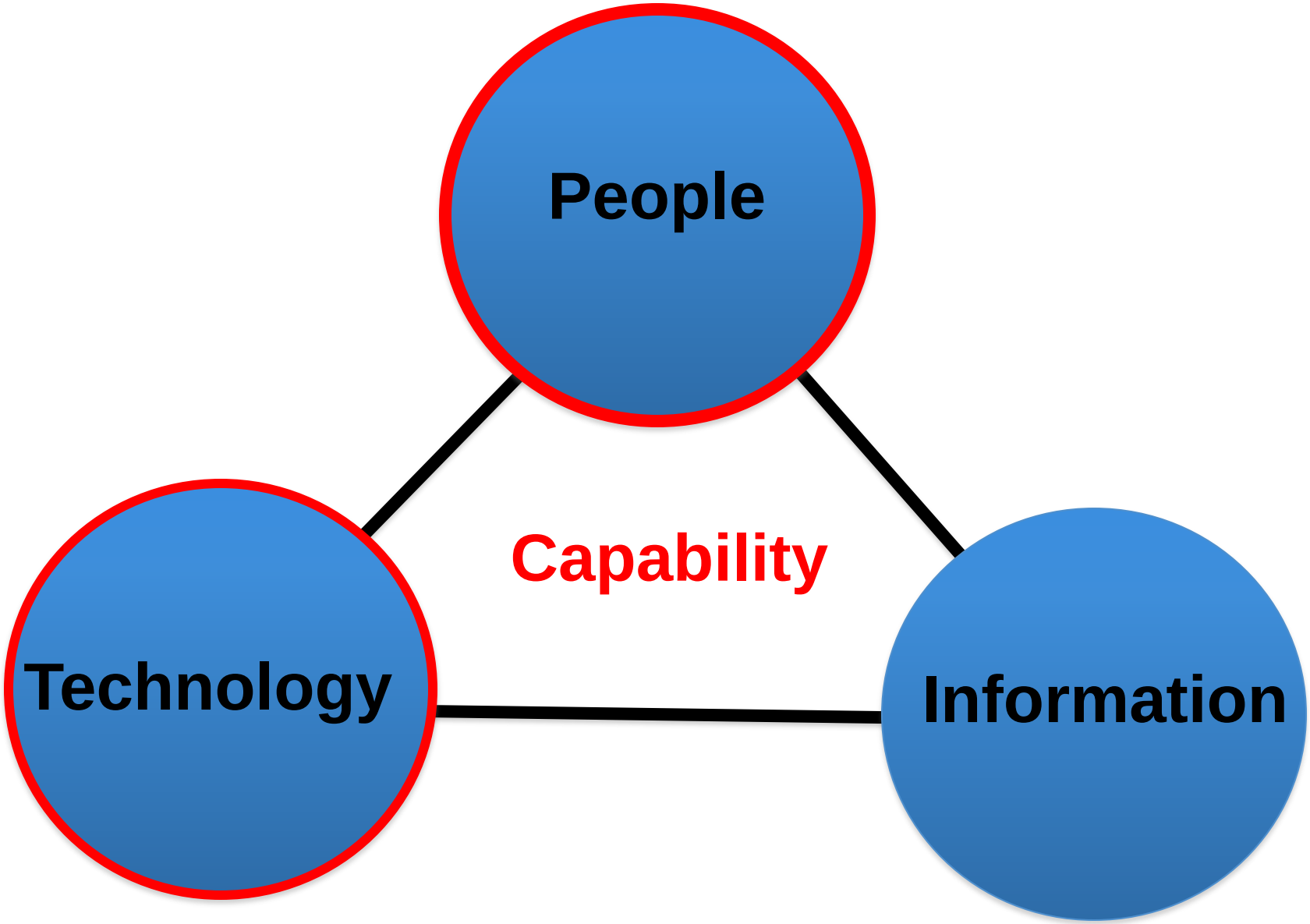
Smilies | Colours | Translation | PasteBin | Minify URL

Menu

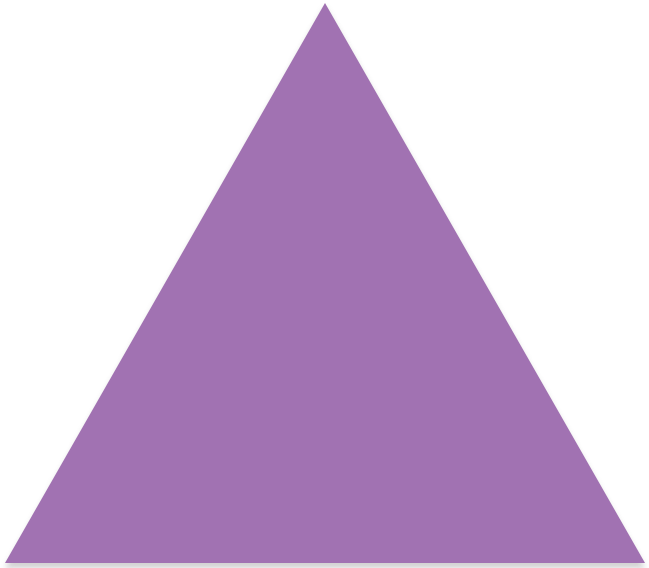



#OpNewBlood
#OpGreenRights
#DDOS
#OpFrance
#OpGlobalBlackout
#Francophone
#OpChina

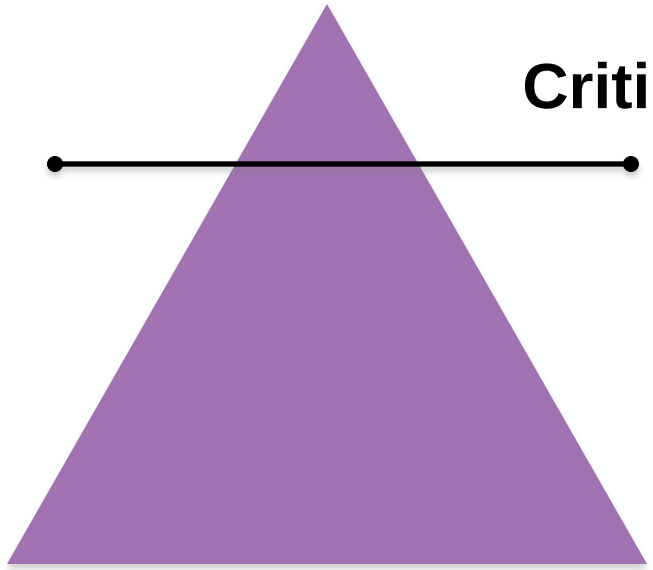

People
Capability
Technology
Information


People
Capability
Technology
Information

Levels of Intelligence product

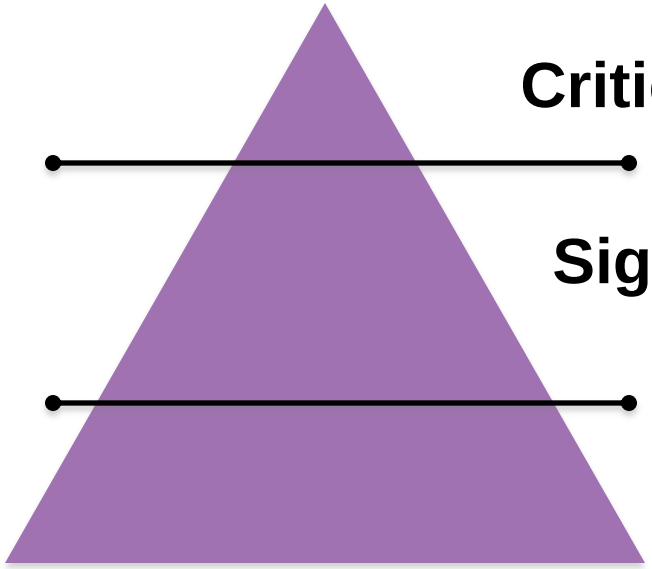


Levels of Intelligence product



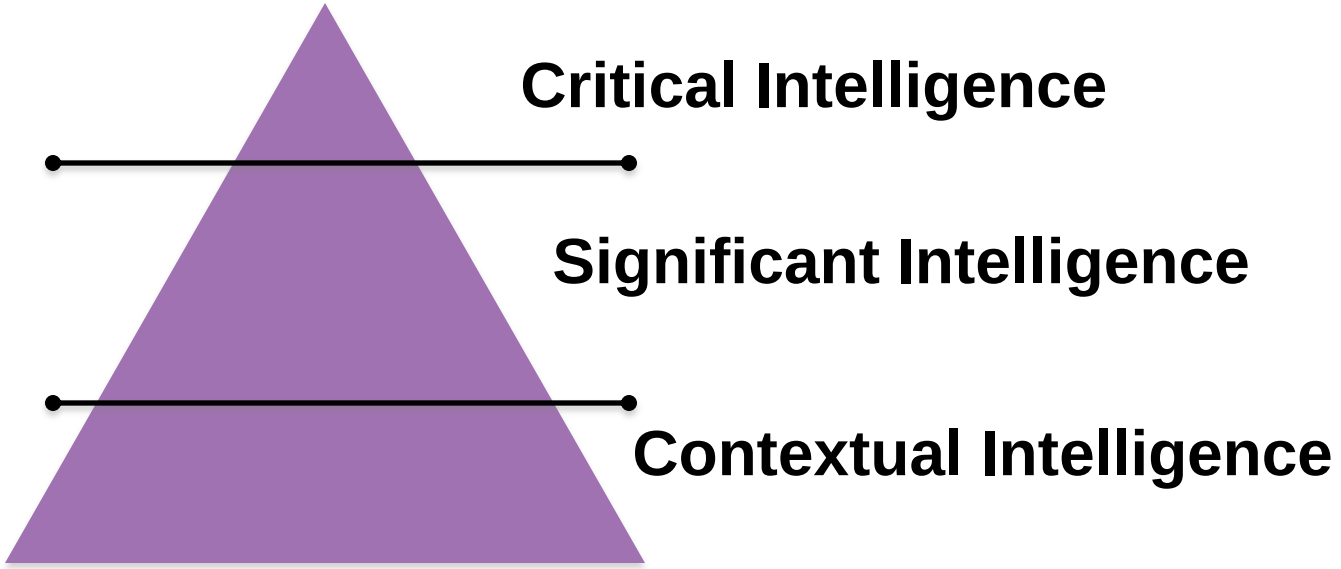
“Mr President the missiles are in flight!”

Levels of Intelligence product



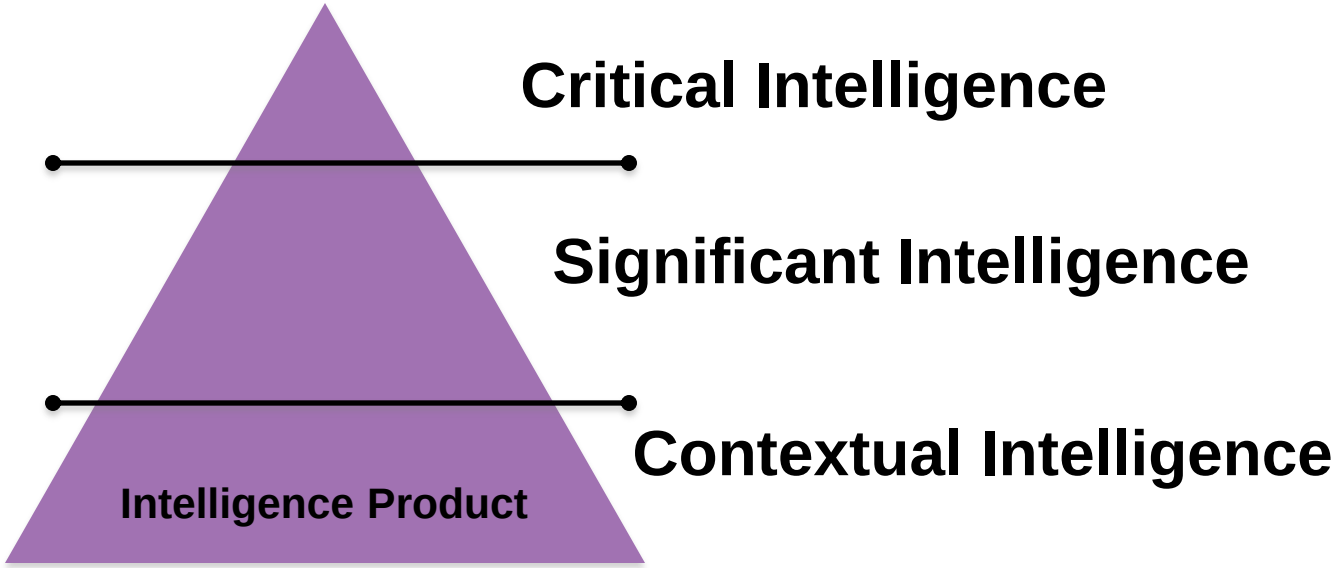
“Iran may be developing a nuclear weapons capability ”

Levels of Intelligence product

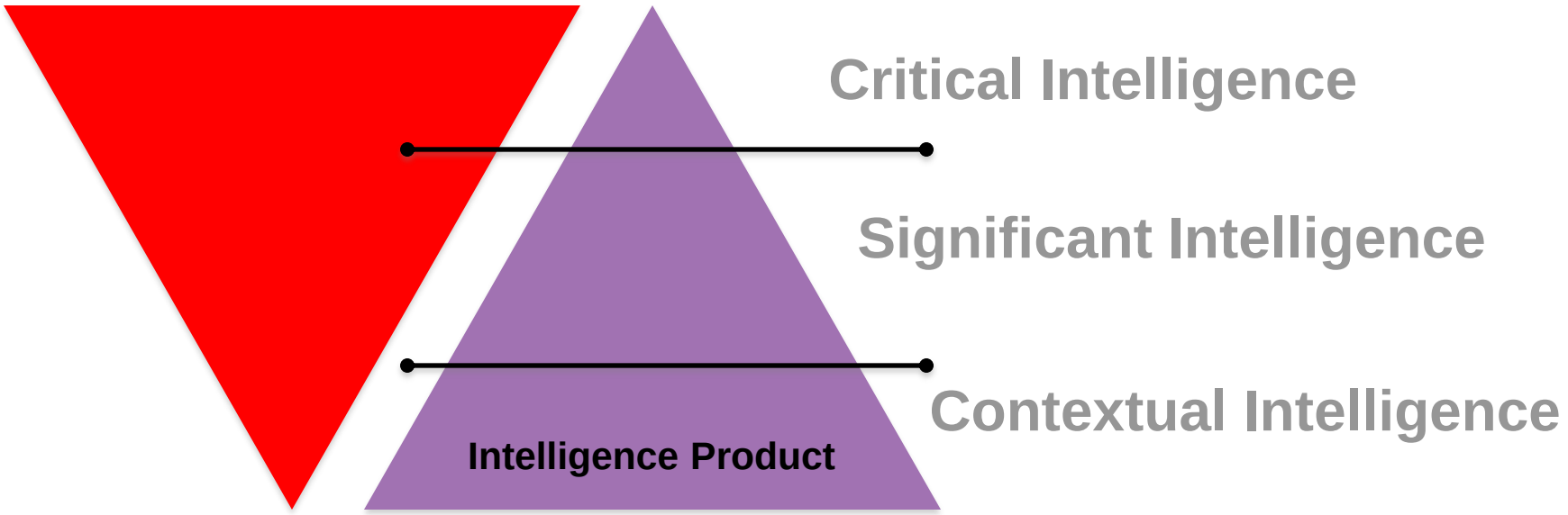


“Country X’s long term political goals could bring us into conflict with them in the next 20 years”

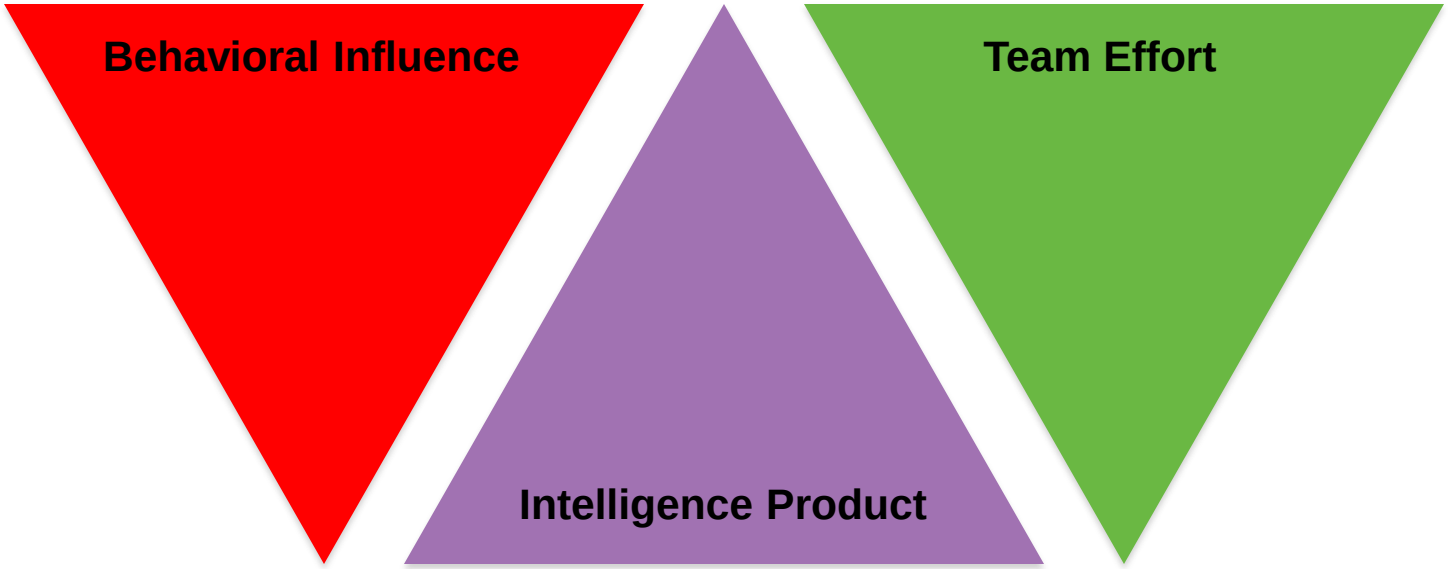
Levels of Intelligence product



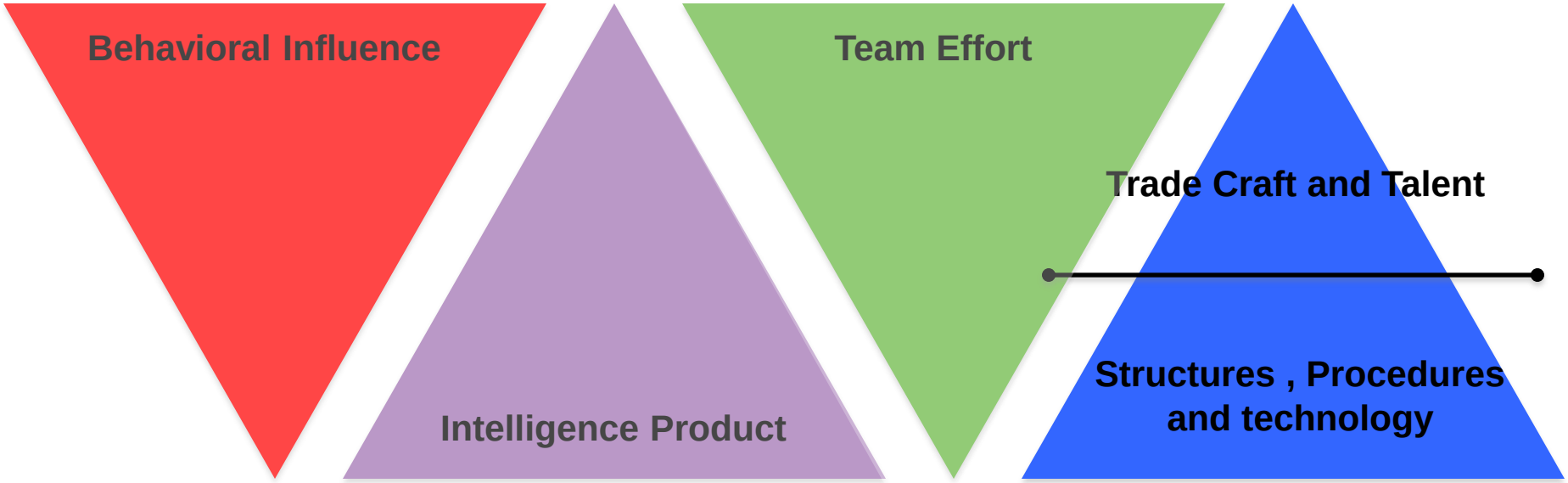
Change In Behavior Within The Decision Maker

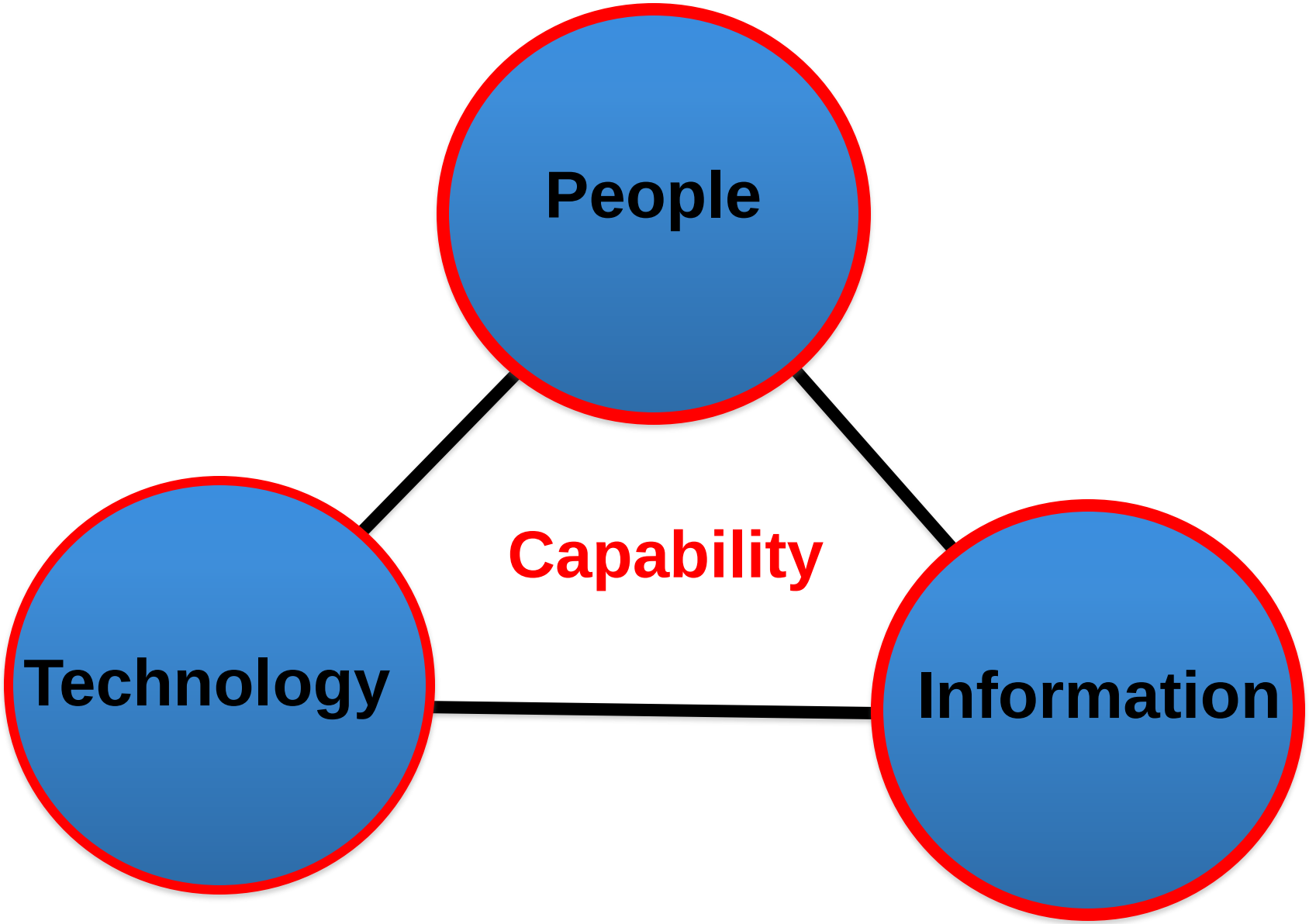


Direct Levels of Intelligence Team Effort



Technical Automaton VS Human Talent




People
Capability
Technology
Information

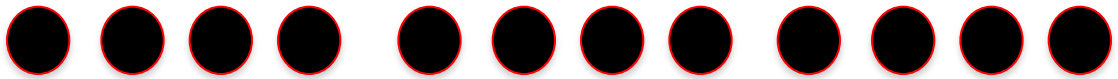
Intelligence

Information

Data

Intelligence

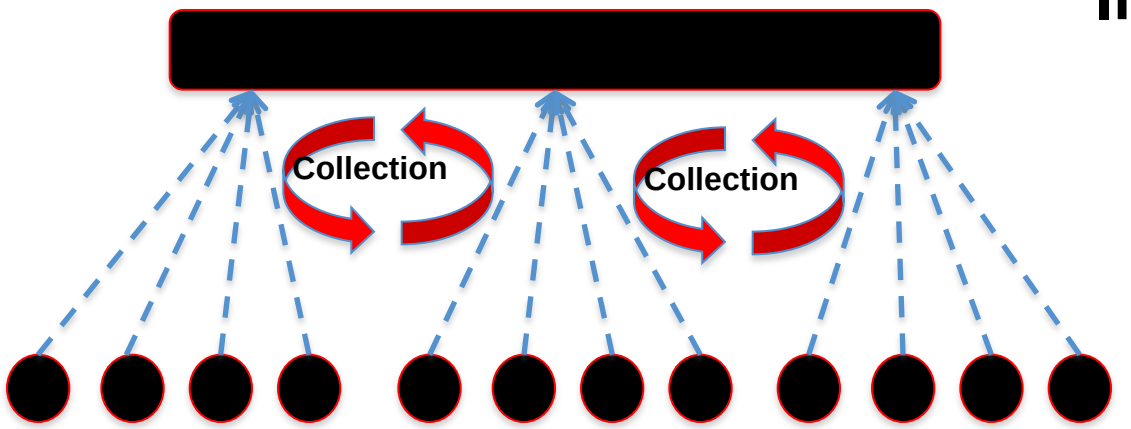
Information



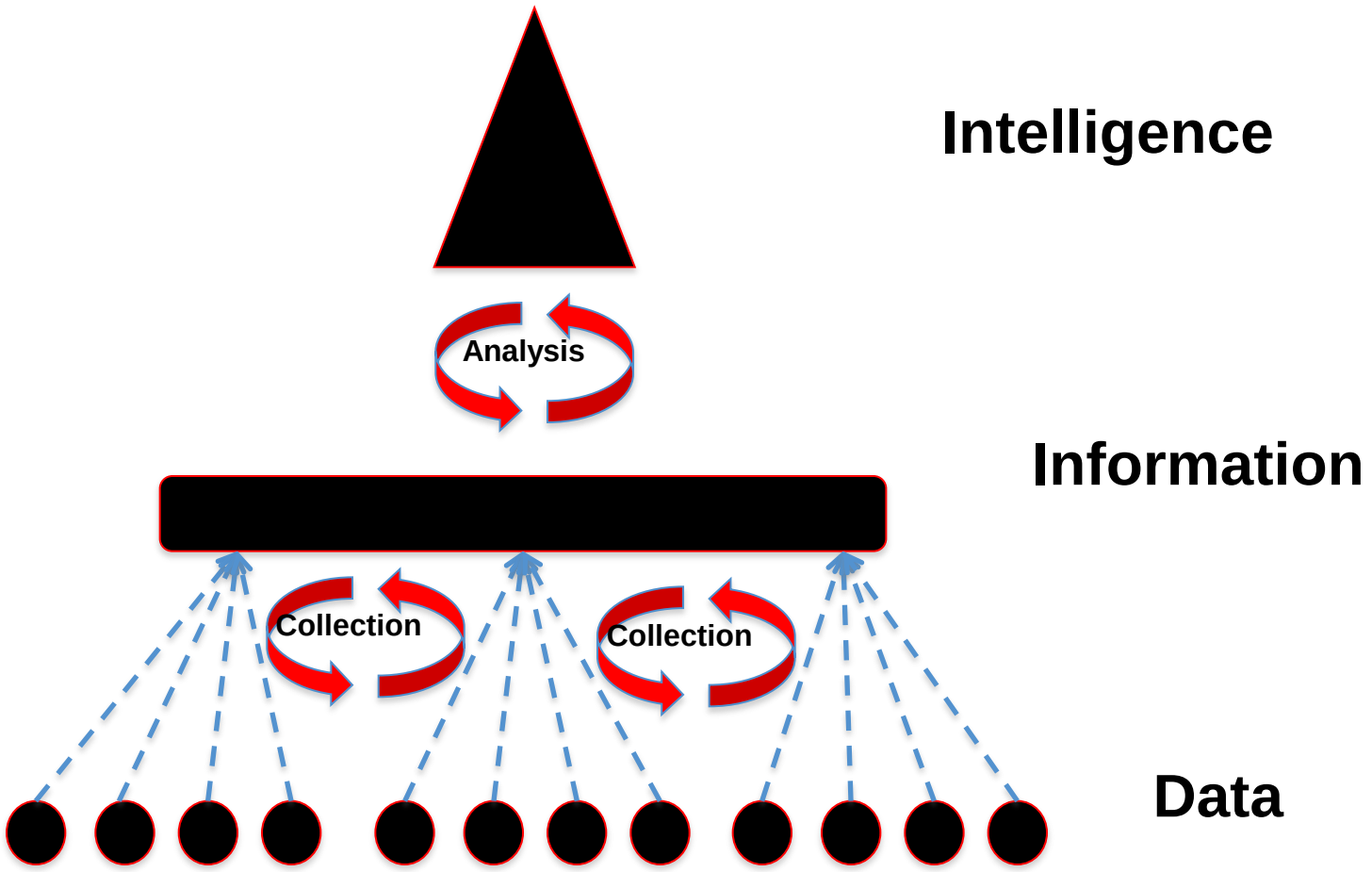
Data

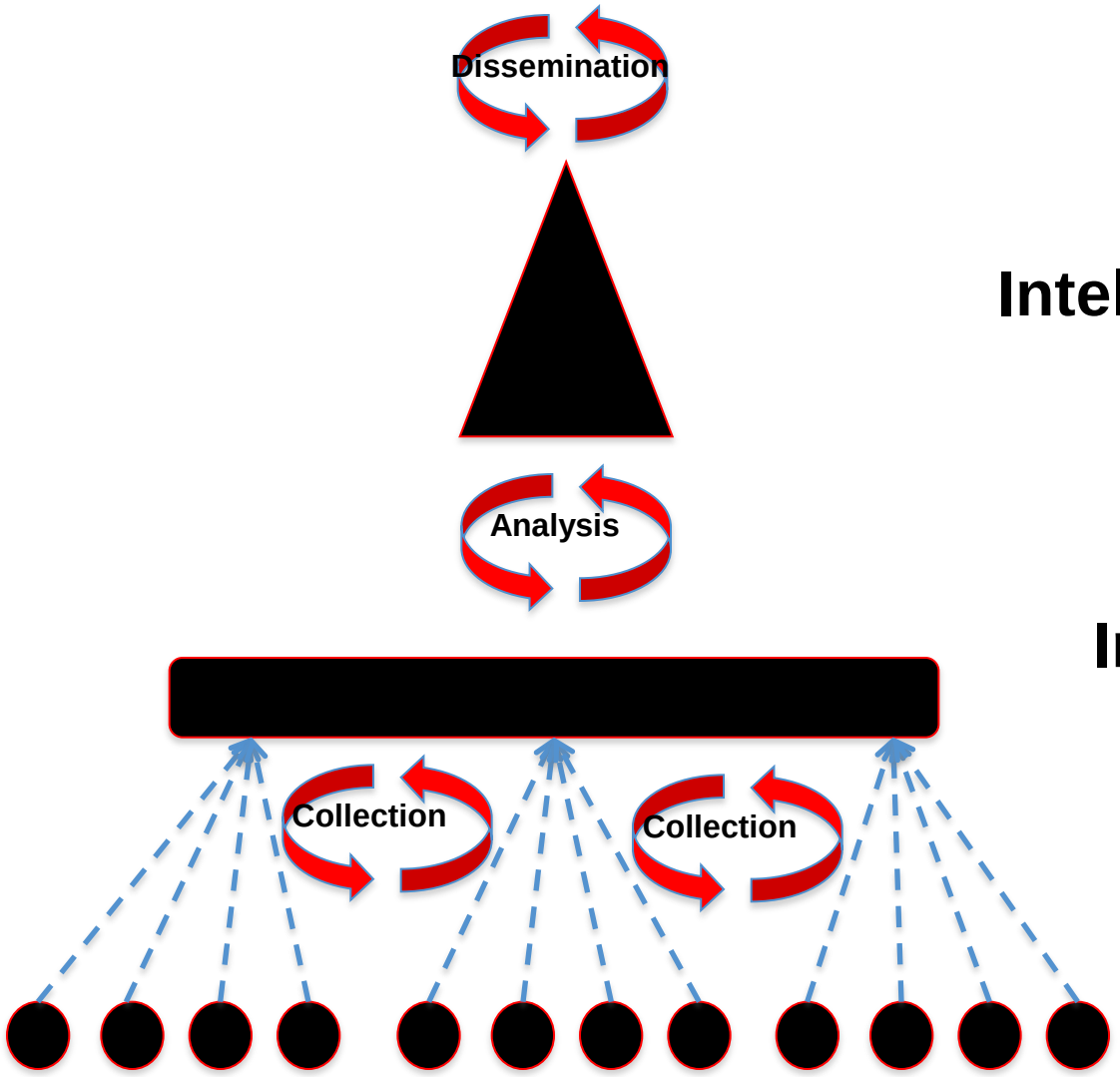
Intelligence

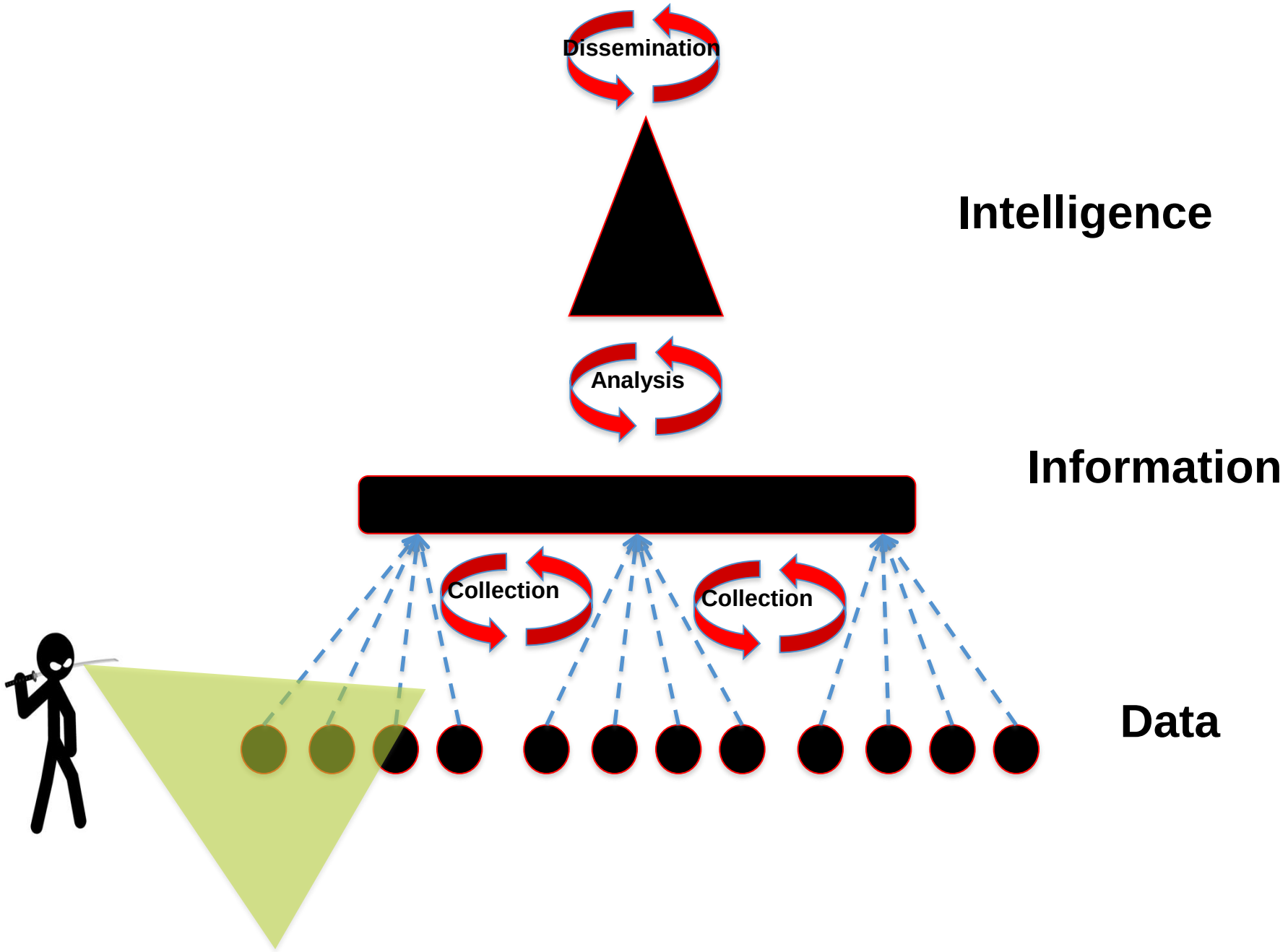
Information

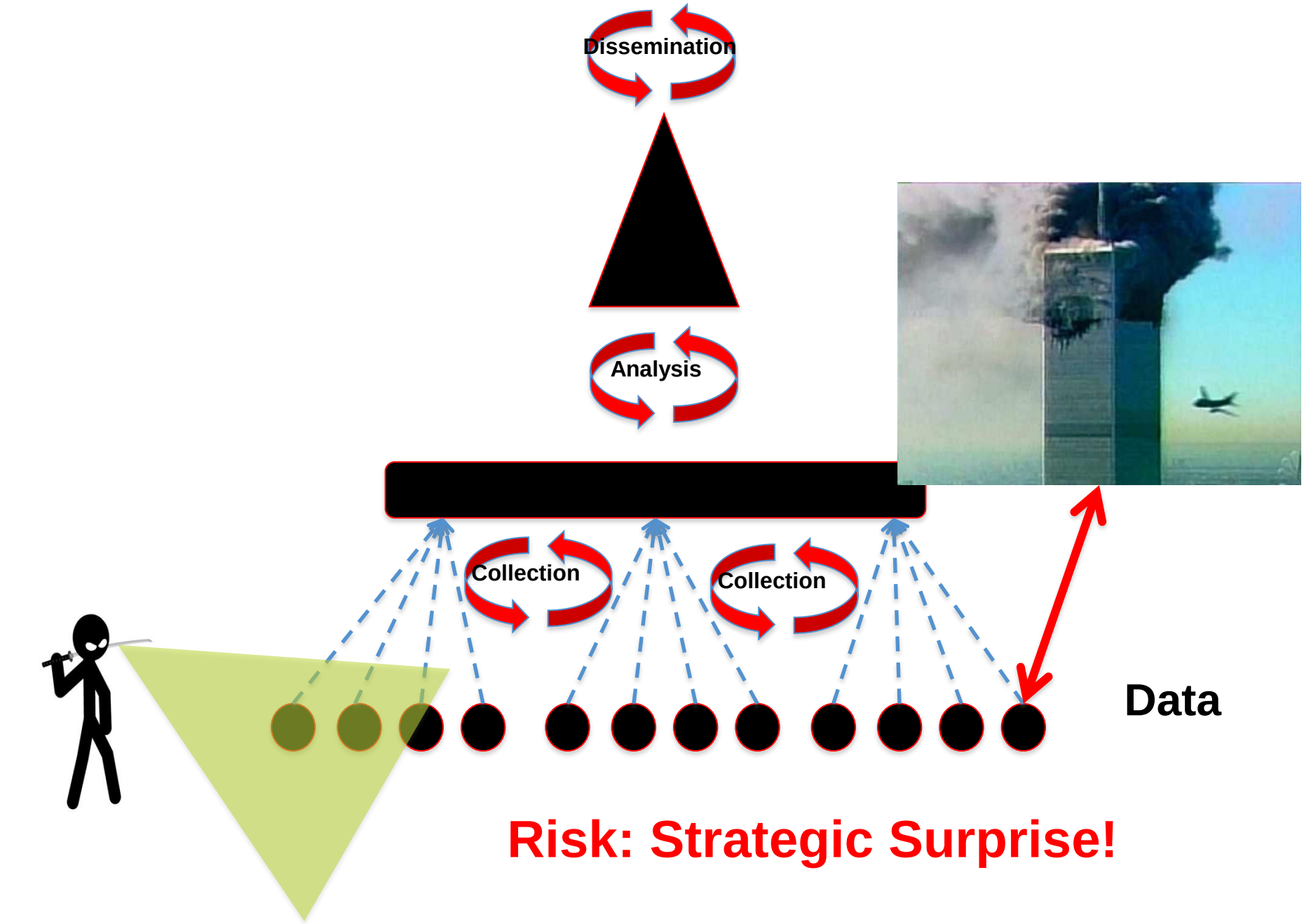


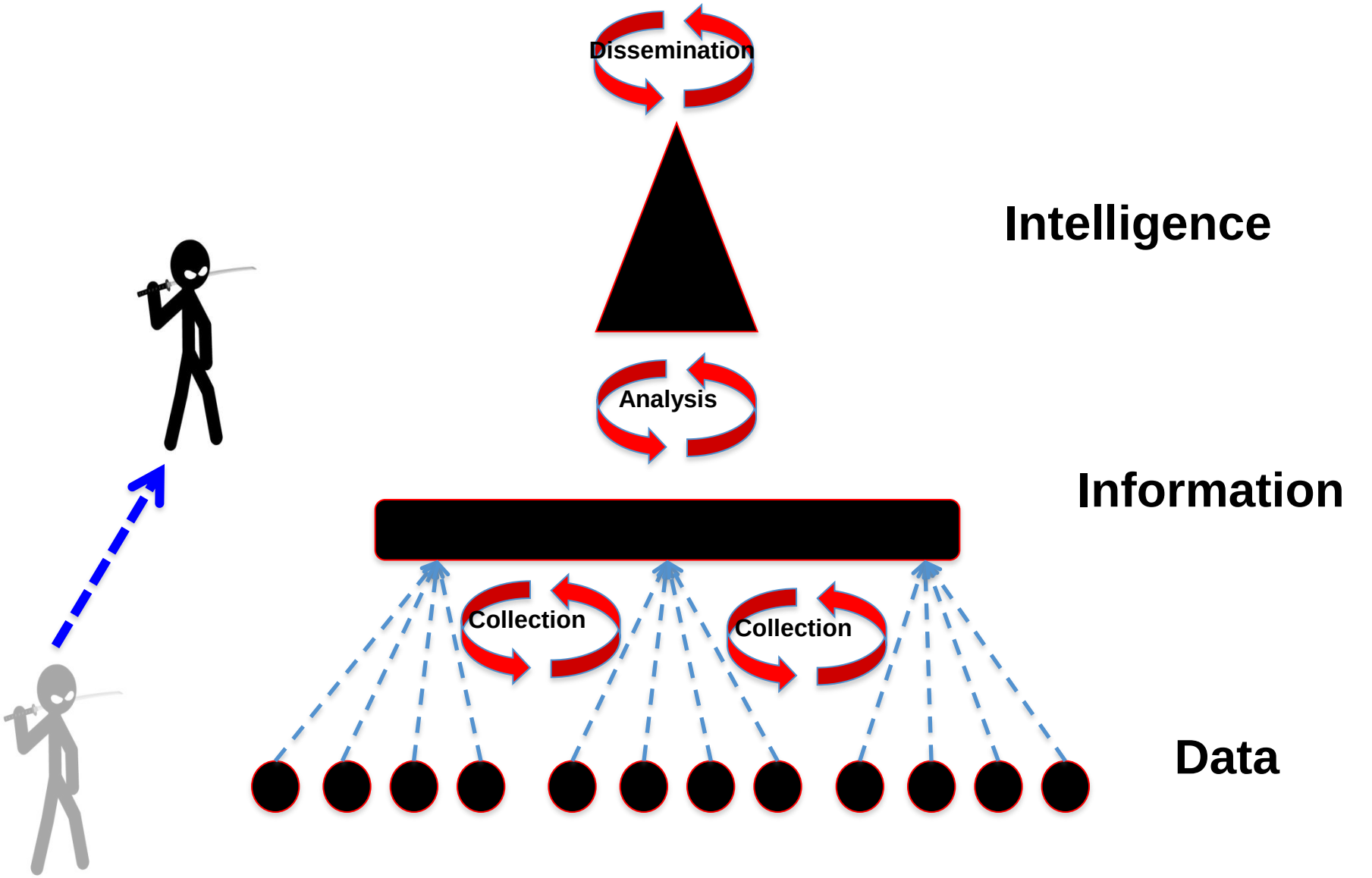
Data


Intelligence
Analysis
Information
Collection
Collection
Data

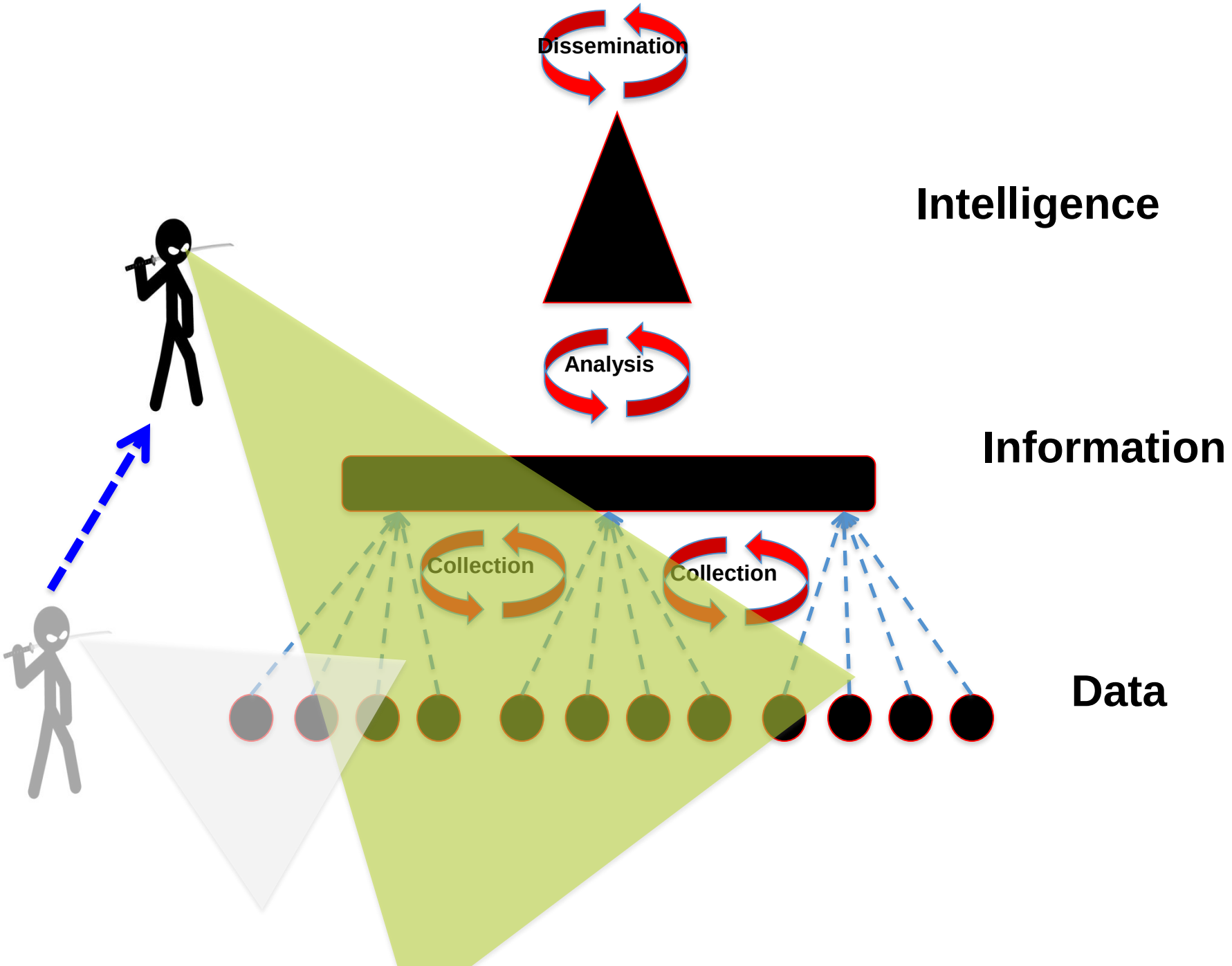

Dissemination
Intelligence
Analysis
Information
Collection
Collection
Data

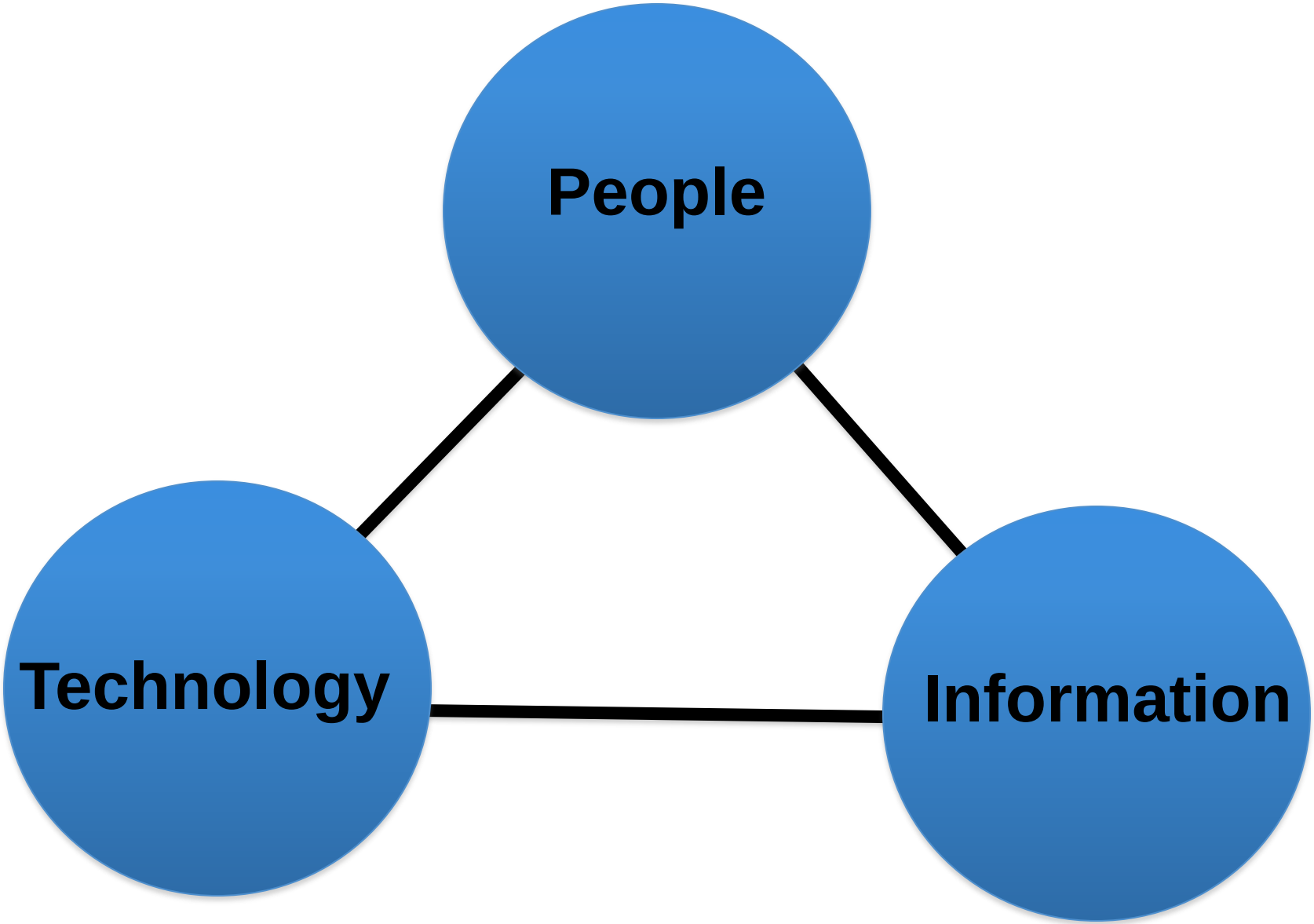

Dissemination
Intelligence
Analysis
Information
Collection
Collection
Data


Dissemination
Analysis
Collection
Collection
Data
Risk: Strategic Surprise!



The Up The Pyramid Principle


Dissemination
Intelligence
Analysis
Information
Collection
Collection
Data


People
Technology
Information

"Why are we even discussing an intelligence capability in the first place?"

"Why are we even discussing an intelligence capability in the first place?"

"Why are we even discussing an intelligence capability in the first place?"

"Why are we even discussing an intelligence capability in the first place?"

- "Is Cyber Threat posing a greater threat than it was 10 years ago?"

"Why are we even discussing an intelligence capability in the first place?"

- "Is Cyber Threat posing a greater threat than it was 10 years ago?"

Contextual Change

"Why are we even discussing an intelligence capability in the first place?"

- "Is Cyber Threat posing a greater threat than it was 10 years ago?"
- **YES**

"Why are we even discussing an intelligence capability in the first place?"

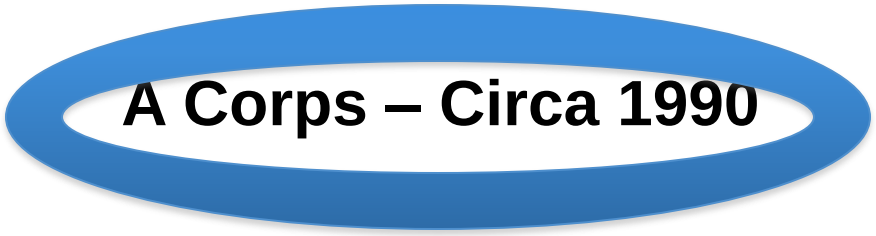
- "Is Cyber Threat posing a greater threat than it was 10 years ago?"
- **YES**
- **BUT**

"Why are we even discussing an intelligence capability in the first place?"

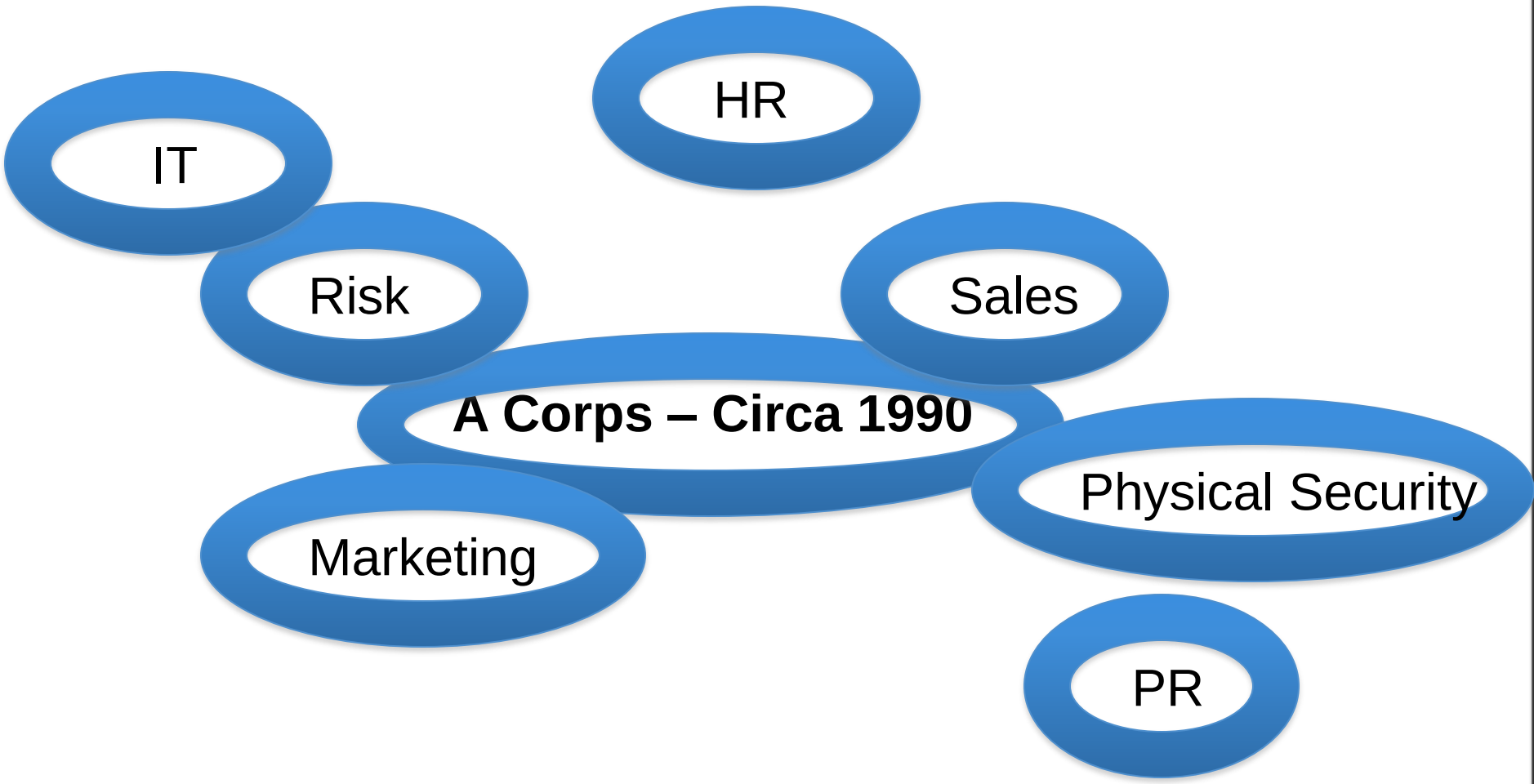
- "Is Cyber Threat posing a greater threat than it was 10 years ago?"
- **YES**
- **BUT**
  - ***Due to the contextual change of the importance of cyber space to Western Society***

Effect on the intelligence team within the wider business context

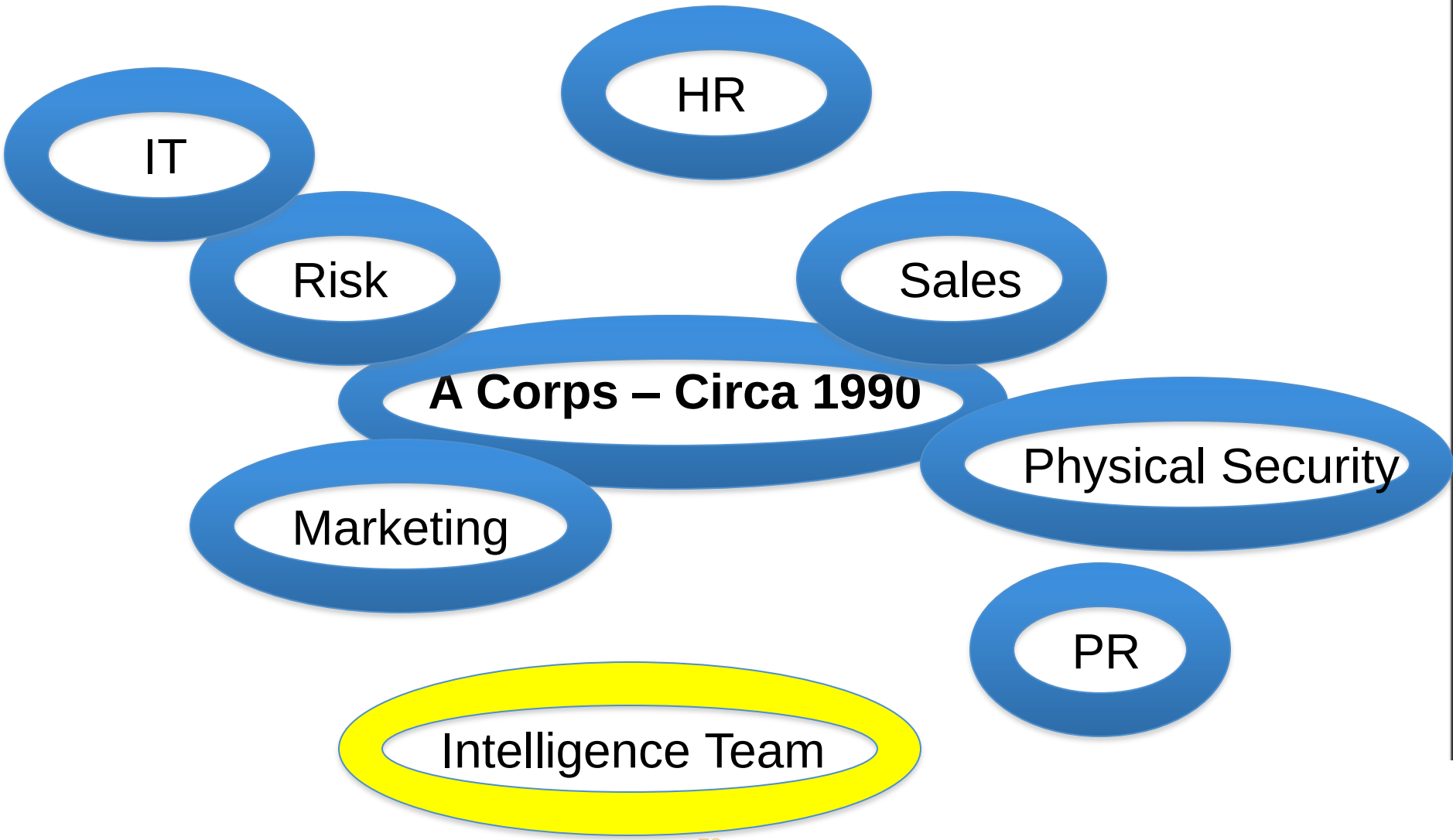
Effect on the intelligence team within the wider business context



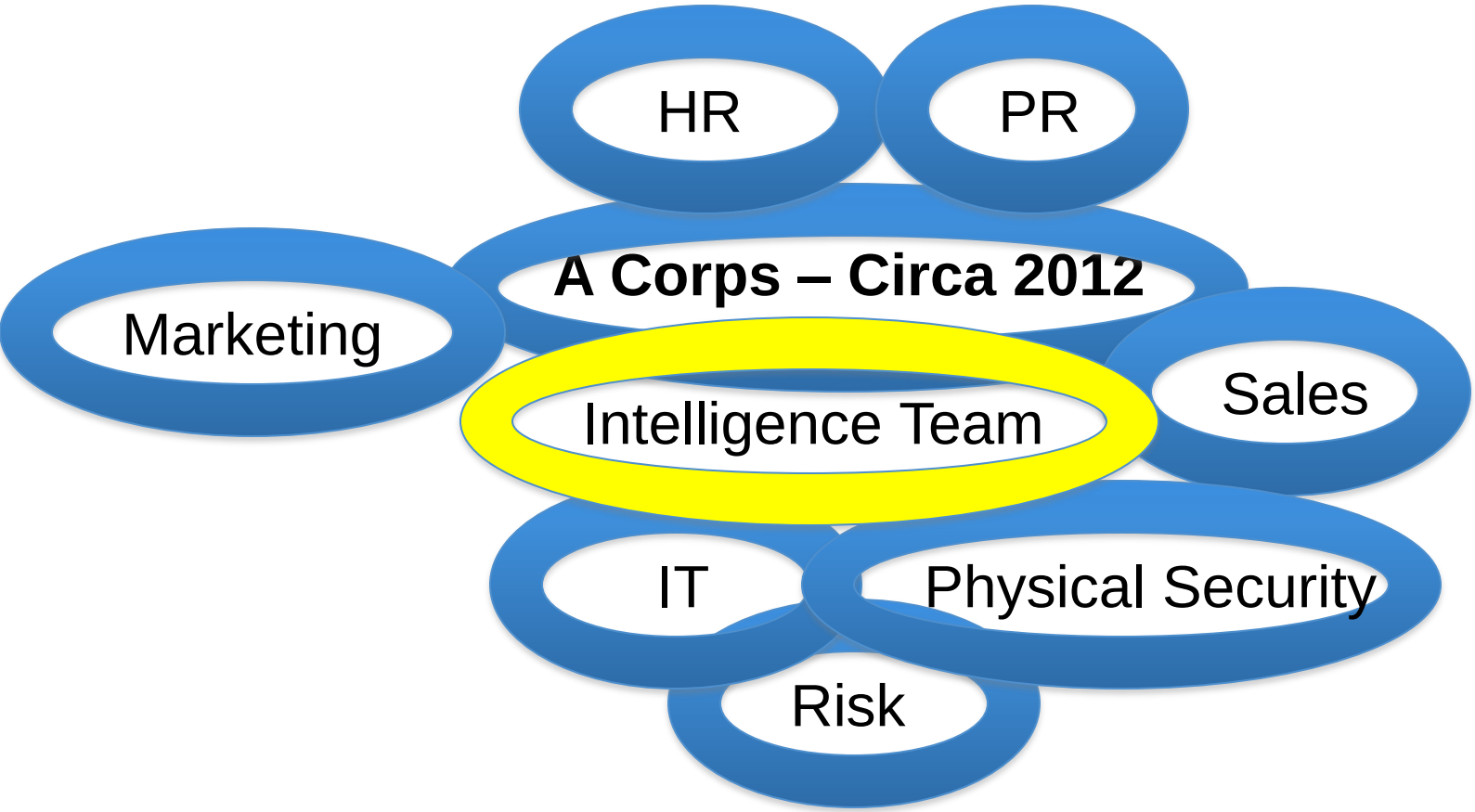
Effect on the intelligence team within the wider business context



Effect on the intelligence team within the wider business context



Effect on the intelligence team within the wider business context



Talk Contents

- Objective
  - Share some thoughts on what a good model for a cyber intelligence team should look like in the private sector
  - Lessons learnt over the past years
- Contents
  1. The socio-technical approach to intelligence team design
  2. The growth of the influence of the intelligence team within the wider business context
  3. Some points to consider – legal and reporting points

Talk Contents

- Objective
  - Share some thoughts on what a good model for a cyber intelligence team should look like in the private sector
  - Lessons learnt over the past years
- Contents
  1. The sociotechnical approach to intelligence team design
  2. The growth of the influence of the intelligence team within the wider business context
  3. Some points to consider – legal and reporting points

جهاد الصومال

@HSMPress_arabic

أخبار حركة الشباب المجاهدين في الصومال - هذه الصفحة غير رسمية

Follow

Text **follow HSMPress_arabic** to your carrier's shortcode

Tweets | Favorites | Following | Followers | Lists

HSMPress_arabic جهاد الصومال
المتحدث الرسمي: إذا لم توقفوا أبناؤكم سوف تقضون أعواما تبكون موتهم وتندمون بشدة حيث لا ينفع الندم.
12 hours ago

HSMPress_arabic جهاد الصومال
المتحدث الرسمي: 850 جندي لن يكون لهم تأثير وقد فشل آلاف من الكينيين، والأثيوبيين، والأوغنديين، والبوروندييين، والمرتزقة الأمريكيين بشكل ذريع.
22 hours ago

HSMPress_arabic جهاد الصومال
المتحدث الرسمي: من معيب على جيبوتي أن تقف مع العدو وتشارك في غزو بلادنا ونحن من قاتلنا من أجل تحريرها
22 hours ago

HSMPress_arabic جهاد الصومال
المتحدث الرسمي الشيخ علي محمود راجي يتحدث إلى إذاعة الأندلس الإسلامية حول قرار جيبوتي إرسال جنود إلى الصومال
22 hours ago

HSMPress_arabic جهاد الصومال
#Welsh: على الغرب أن يعترف بحركة الشباب كالعامل الوحيد القادر على إقامة نظام حكم في #الصومال tinyurl.com/75nfr3x
14 Dec

HSMPress_arabic جهاد الصومال
تحديث: هجوم الليلة الماضية على تابتو إستمر لساعة وكانت نتيجته مقتل 3 جنود كينيين. وتم إشعال مخزن الذخيرة كذلك.
13 Dec

About @HSMPress_arabic

46	1	40	0
Tweets	Following	Followers	Listed

https://www.facebook.c

facebook

Email

Password

Log In

Keep me logged in

Forgot your password?

Muslim Defence League (MDL) – United We Stand, Divided We Fall is on Facebook.

To connect with Muslim Defence League (MDL) – United We Stand, Divided We Fall, sign up for Facebook today.

Sign Up Log In

Muslim Defence League (MDL) – United We Stand, Divided We Fall

Like

15,829 likes · 1,508 talking about this

Political Organization

Fighting against racism, fascism and oppression. We welcome everyone from all faiths and backgrounds.
http://muslimdefenceleague.wordpress.com/

15,829

Quran and Hadith prove Islam's
Quran and Hadith Islam's Opposition

1

About Photos Likes Events Notes 3

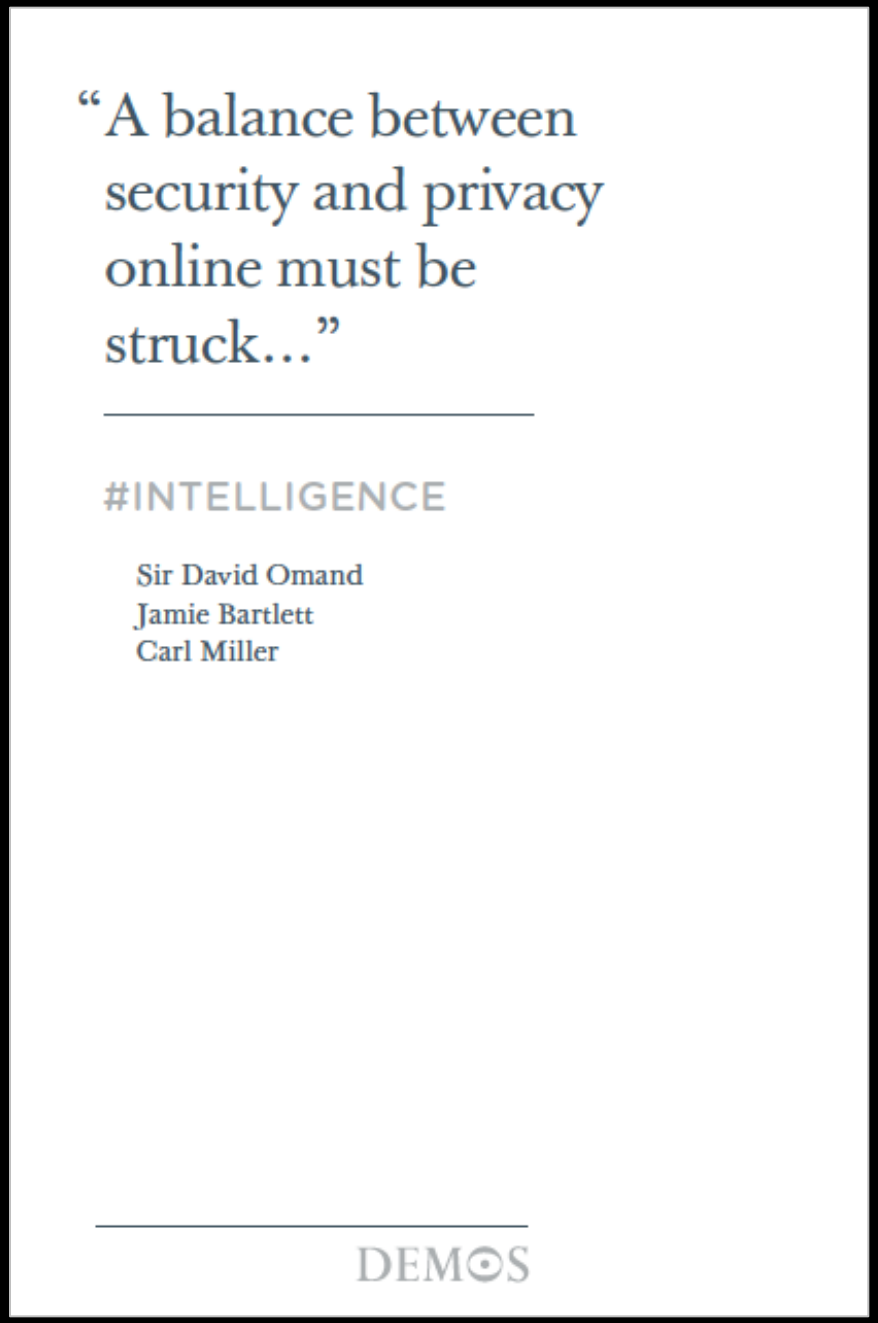
Highlights

"A balance between security and privacy online must be struck…"

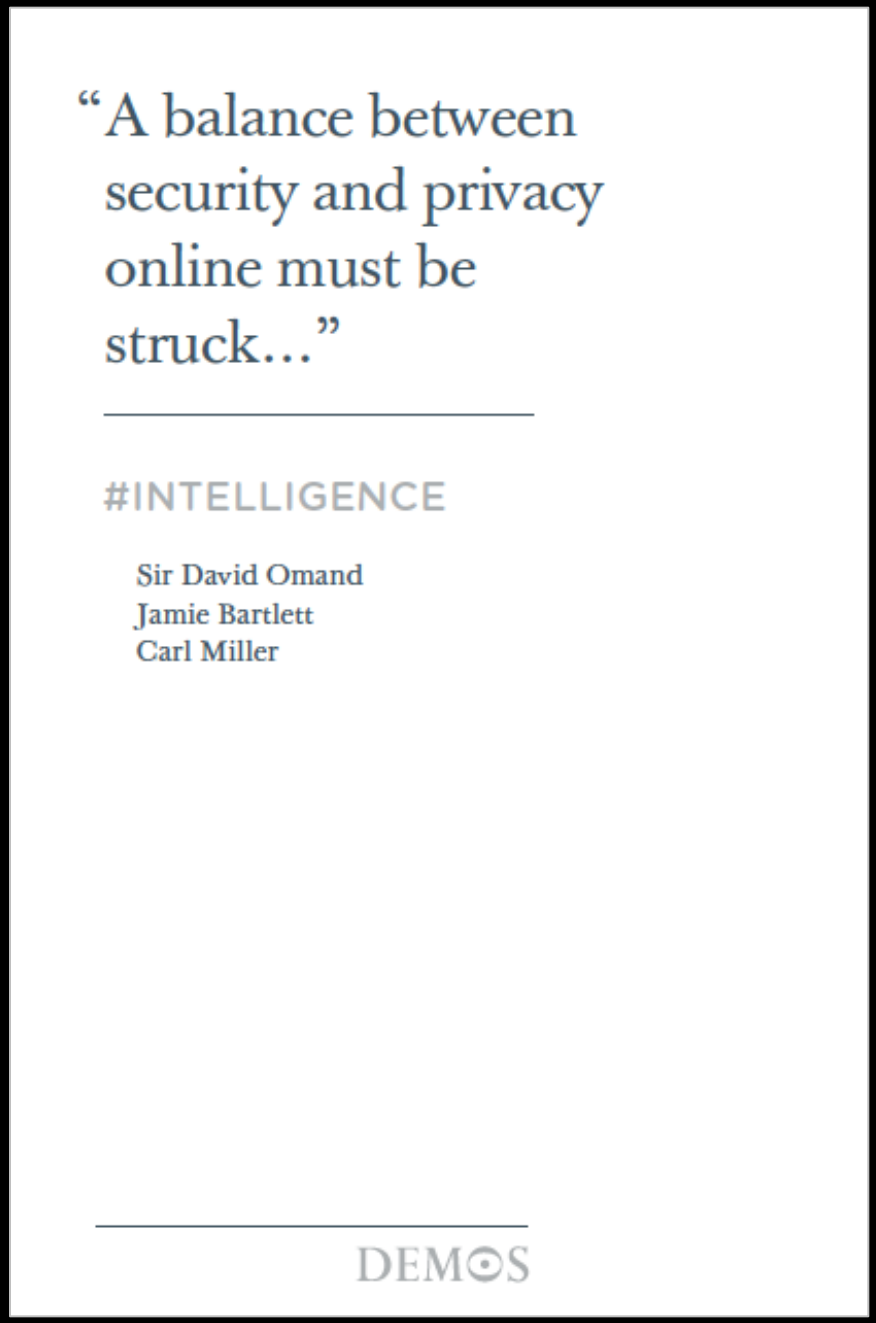
#INTELLIGENCE

Sir David Omand
Jamie Bartlett
Carl Miller

DEMOS



- **Social Media Intelligence "SOCMINT"**
- **"SOCMINT is not yet capable of making a decisive contribution to public security and safety."**
- **"SOCMINT does not fit easily into the existing systems we have developed to ensure intelligence collected can be confidently acted on."**



- **Social Media Intelligence "SOCMINT"**
- **"SOCMINT is not yet capable of making a decisive contribution to public security and safety."**
- **"SOCMINT does not fit easily into the existing systems we have developed to ensure intelligence collected can be confidently acted on."**

- **“SOCMINT does not fit easily into the existing systems we have developed to ensure intelligence collected can be confidently acted on.”**

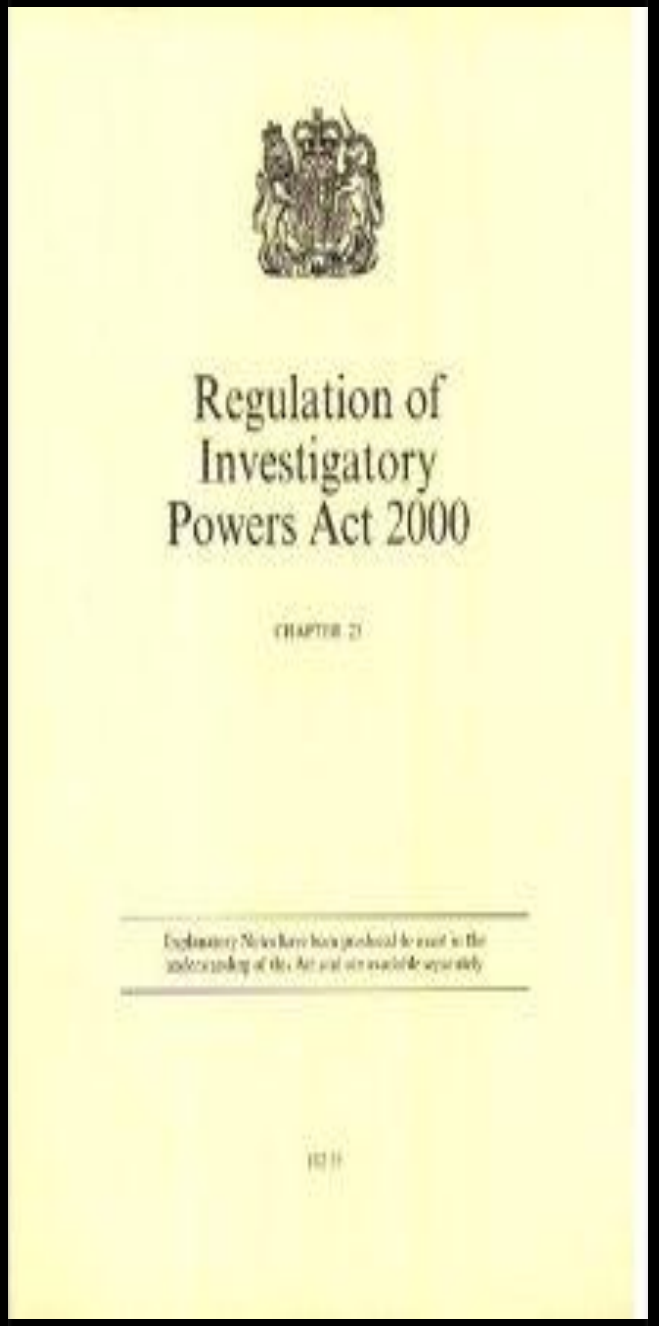
- **“SOCMINT does not fit easily into the existing systems we have developed to ensure intelligence collected can be confidently acted on.”**

"A balance between security and privacy online must be struck…"

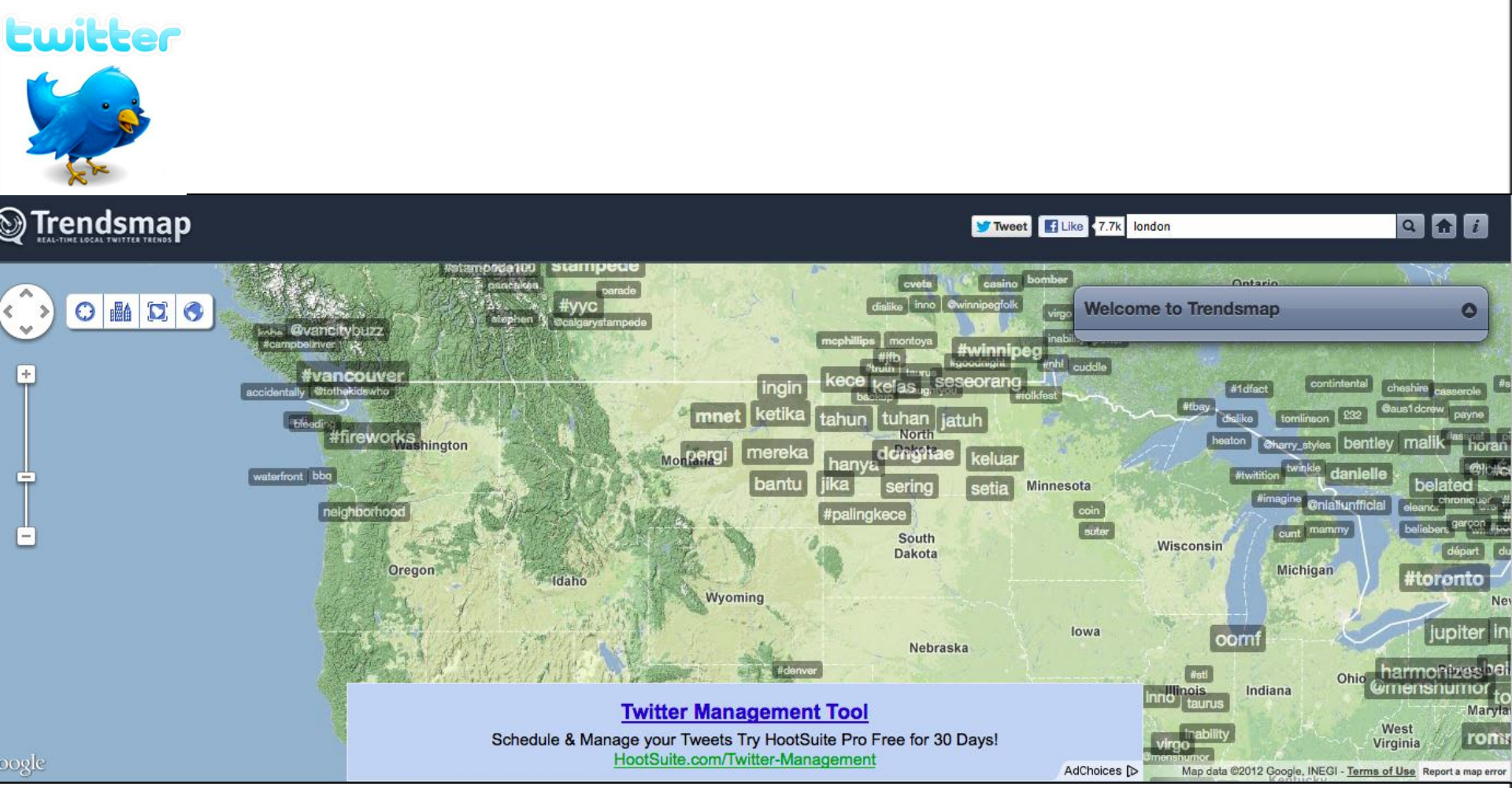
#INTELLIGENCE

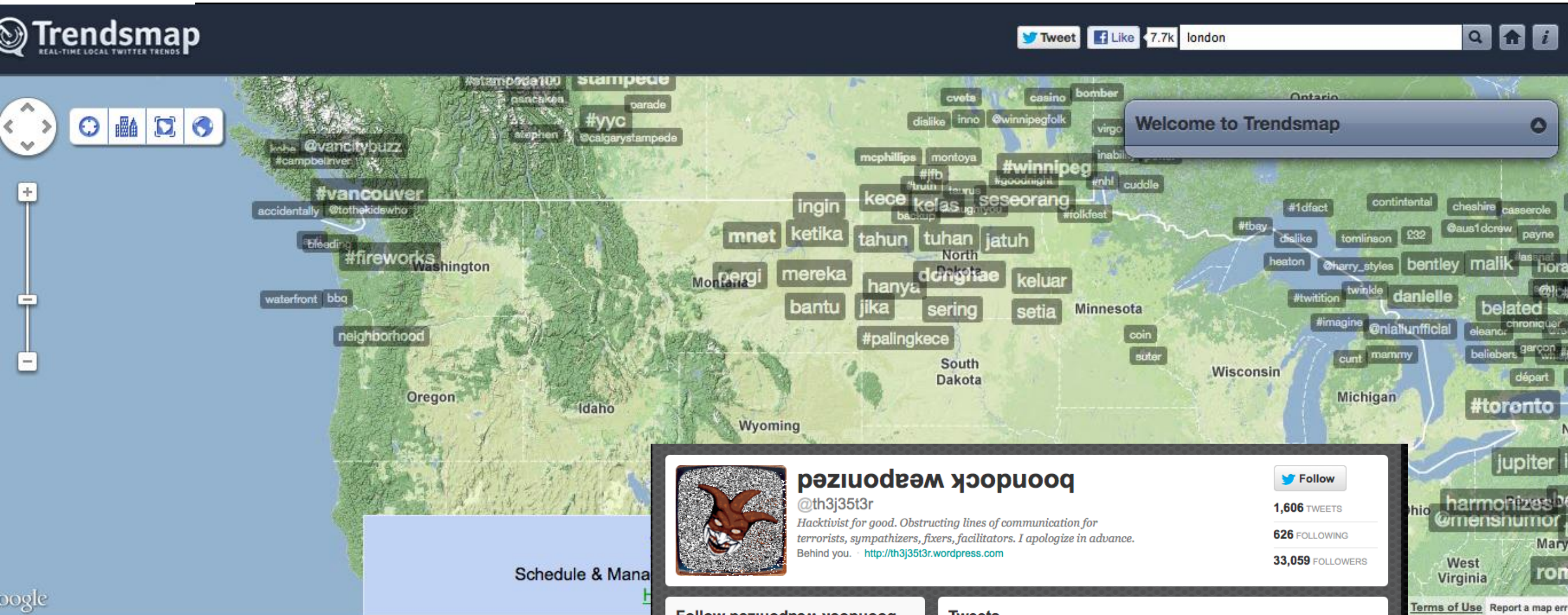
Sir David Omand
Jamie Bartlett
Carl Miller

DEMOS

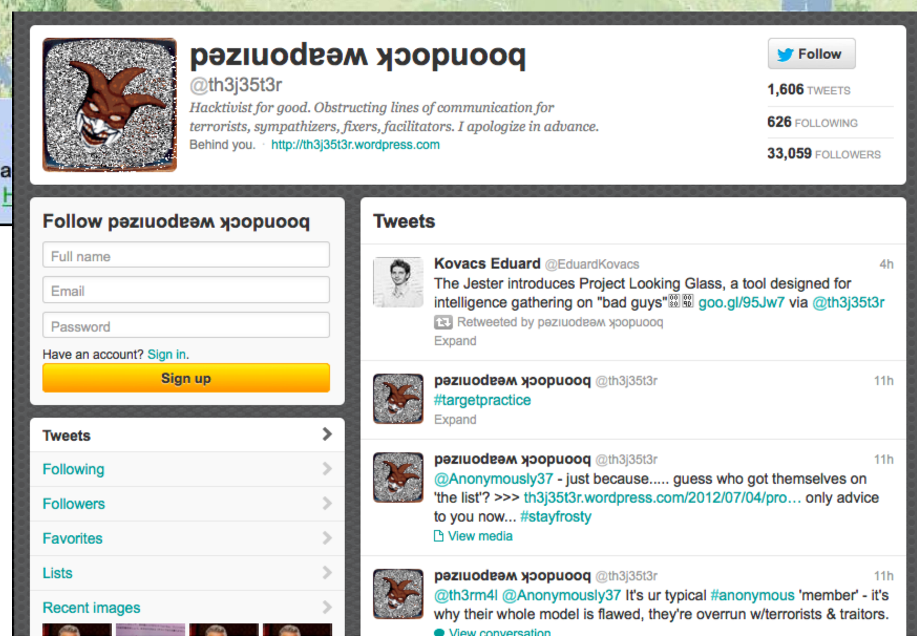


twitter

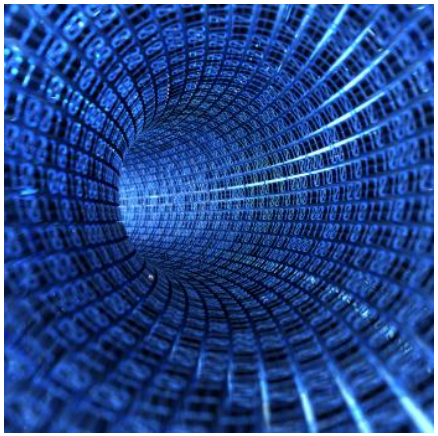

twitter
Trendsmap
REAL-TIME LOCAL TWITTER TRENDS
Tweet
Like
7.7k
london
Welcome to Trendsmap
#vancouver
#fireworks
#yyc
#winnipeg
#toronto
#palingkece
ingin
kece
kelas
seseorang
mnet
ketika
tahun
tuhan
jatuh
mereka
bantu
jika
sering
setia
keluar
danielle
belated
bentley
malik
oomf
jupiter
harmonizes
Washington
Oregon
Idaho
Wyoming
Nebraska
Minnesota
Wisconsin
Michigan
Indiana
Ohio
West Virginia
South Dakota
North Dakota
Twitter Management Tool
Schedule & Manage your Tweets Try HootSuite Pro Free for 30 Days!
HootSuite.com/Twitter-Management
AdChoices
Map data ©2012 Google, INEGI - Terms of Use
Report a map error



Trendsmap
REAL-TIME LOCAL TWITTER TRENDS
Tweet
Like
7.7k
london
Welcome to Trendsmap
#vancouver
@vancitybuzz
#fireworks
#yyc
@calgarystampede
#winnipeg
#toronto
Washington
Oregon
Idaho
Montana
Wyoming
North Dakota
South Dakota
Minnesota
Wisconsin
Michigan
West Virginia
Schedule & Mana
Terms of Use
Report a map error



pǝzıuodǝɐʍ ʞɔopuooq
@th3j35t3r
Hacktivist for good. Obstructing lines of communication for terrorists, sympathizers, fixers, facilitators. I apologize in advance.
Behind you. · http://th3j35t3r.wordpress.com
Follow
1,606 TWEETS
626 FOLLOWING
33,059 FOLLOWERS
Follow pǝzıuodǝɐʍ ʞɔopuooq
Full name
Email
Password
Have an account? Sign in.
Sign up
Tweets
Following
Followers
Favorites
Lists
Recent images
Tweets
Kovacs Eduard @EduardKovacs 4h
The Jester introduces Project Looking Glass, a tool designed for intelligence gathering on "bad guys" goo.gl/95Jw7 via @th3j35t3r
Retweeted by pǝzıuodǝɐʍ ʞɔopuooq
Expand
pǝzıuodǝɐʍ ʞɔopuooq @th3j35t3r 11h
#targetpractice
Expand
pǝzıuodǝɐʍ ʞɔopuooq @th3j35t3r 11h
@Anonymously37 - just because..... guess who got themselves on 'the list'? >>> th3j35t3r.wordpress.com/2012/07/04/pro... only advice to you now... #stayfrosty
View media
pǝzıuodǝɐʍ ʞɔopuooq @th3j35t3r 11h
@th3rm4l @Anonymously37 It's ur typical #anonymous 'member' - it's why their whole model is flawed, they're overrun w/terrorists & traitors.
View conversation



Public Place?
Private Place?
Something Else?

Expectation of privacy?

1st Question

2nd Question

- **“SOCMINT does not fit easily into the existing systems we have developed to ensure intelligence collected can be confidently acted on.”**

Some Thoughts on SOCMINT

- SOCMINT is a combination of two intelligence disciplines
  - Signals Intelligence (SIGINT): the communication element of the medium
  - Human Intelligence (HUMINT): the message element of the medium
- The 5 x 5 x 5 intelligence grading system is ideal for SOCMINT reporting
- ***SO WHAT?: If done write then OSINT based intelligence can have a far greater penetration rate within an organization than other closed sources of inelligence***

5x5x5 according to the NIM

5x5x5 according to the NIM

Intel Evaluation

1 – Known to be true without reservation

2 – Information known personally to the source but not to the reporting agent

3 – Information is not known personally to the source but there is corroboration by information already recorded

4 – Information that is not known to the source and cannot be corroborated

5 – Information that is suspected to be false

5x5x5 according to the NIM

Source Evaluation

A – Always reliable

B – Mostly reliable

C – Sometimes reliable

D – Unreliable

E – Previously untested

5x5x5 according to the NIM

Handling code

Code 1 – Permits dissemination to other law enforcement and prosecuting agencies (such as Benefits Agency) including agencies abroad where there are sufficient safeguards to protect the rights of individuals.

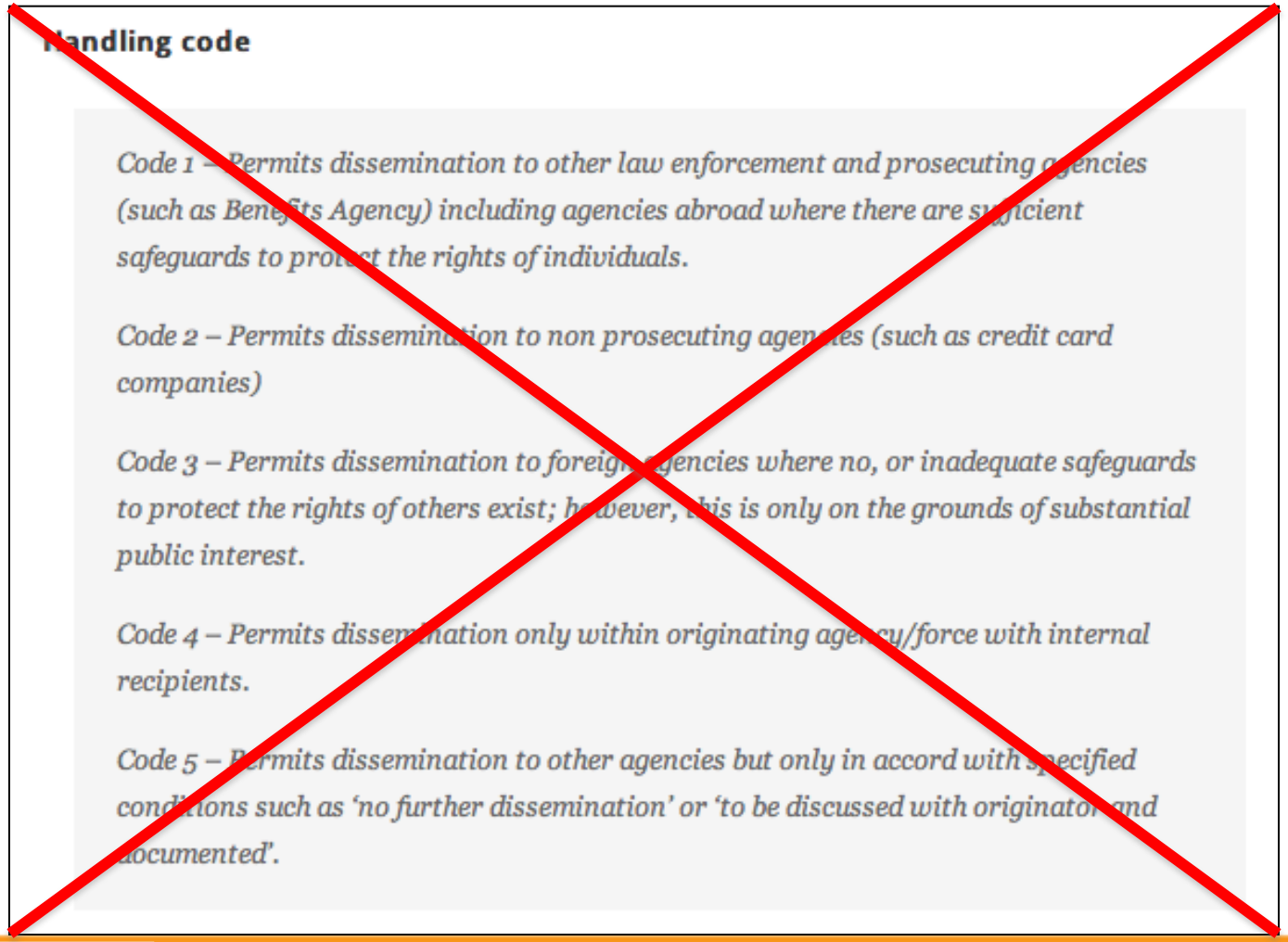
Code 2 – Permits dissemination to non prosecuting agencies (such as credit card companies)

Code 3 – Permits dissemination to foreign agencies where no, or inadequate safeguards to protect the rights of others exist; however, this is only on the grounds of substantial public interest.

Code 4 – Permits dissemination only within originating agency/force with internal recipients.

Code 5 – Permits dissemination to other agencies but only in accord with specified conditions such as 'no further dissemination' or 'to be discussed with originator and documented'.

5x5x5 according to the NIM



Handling code

Code 1 – Permits dissemination to other law enforcement and prosecuting agencies (such as Benefits Agency) including agencies abroad where there are sufficient safeguards to protect the rights of individuals.

Code 2 – Permits dissemination to non prosecuting agencies (such as credit card companies)

Code 3 – Permits dissemination to foreign agencies where no, or inadequate safeguards to protect the rights of others exist; however, this is only on the grounds of substantial public interest.

Code 4 – Permits dissemination only within originating agency/force with internal recipients.

Code 5 – Permits dissemination to other agencies but only in accord with specified conditions such as 'no further dissemination' or 'to be discussed with originator and documented'.

5x5 example

	1/ A	2/ B	3/ C	4/ D	5/ E
Intel Evaluation			●		
Source Evaluation				●	

Grade: Not know to the source but externally corroborated, Unreliable

Some concluding though on Open Source Intelligence

- OSINT Is not for the “new guy”
- Established models of best practice in other intelligence disciplines

Final concluding point on developing a cyber intelligence capability

Final concluding point on developing a cyber intelligence capability

- **“If today is the information age then tomorrow will be the intelligence age”**


Questions?